MASTEROPPGAVE

Emnekode:	Navn på kandidat:
BE323E	Benedicte Bjartland - 168

Norske virksomheters samarbeid med politiet – en studie av hvilke faktorer som påvirker norske virksomheters samarbeid med politiet i forbindelse med datakriminalitet

Dato: 25.05.22 Totalt antall sider: 170

NORD universitet

www.nord.no

Abstract

The ongoing digitalization of our society brings about a great deal of opportunities and advantages, from which most of us benefit. However, it also generates a new variety of vulnerabilities, of which criminals and the like exploit. Norwegian companies experience less serious cyberattacks daily. Within the last few years some companies have also found themselves victims of serious cybercrime, for instance cyberattacks with subsequent encryption of data and ransom claims. Consequently, Norwegian companies are subjected to new requirements within security and preparedness, while the police are challenged in their ability to prevent, avert, handle, and investigate this type of cybercrime. Neither sectors can face these challenges alone, and a well-functioning private-public collaboration is crucial to maintain a necessary level of social security in our society. I based this master thesis on human and organizational factors that affect the collaboration between Norwegian companies and the police in preventing cybercrime, with the following thesis question: *What factors affect Norwegian companies' collaboration with the police in preventing and handling cybercrime?*

The literature reviewed focuses on traditional theoretical perspectives regarding man-made disasters, organizational accidents, high reliability organizations and security culture, accompanied by more recent international research within the field of cyber security. The research focuses on collaboration between private sectors and public authorities, in a digital context where cybercrime poses a serious threat to Norwegian companies. In addition, I have reviewed several public documents published by Norwegian authorities in a quest to pinpoint the responsibilities of the police in the digital landscape, as well as investigate Norwegian authorities' approach to challenges related to cybercrime.

The study was conducted as a descriptive multiple-case study with participants from two different sections. The first section represents key personnel from Norwegian companies in the realm of digital security and preparedness, as well as potential collaboration with the police. The second section represents employees within the Norwegian police, other public authorities, and private security companies who focus on cyber security and -crime. Data was collected through a qualitative method including elements from the grounded theory and the SDI-model. I conducted a total of 18 in-depth interviews distributed between the two sections. The interviews were transcribed before all data material was coded and categorized by using the analysis program NVivo. After processing the material, I was left with the following four main categories of my thesis: "The Norwegian police and cybercrime", "The work being done

on security and preparedness within Norwegian companies", "The nature of cybercrime" and "External factors". These main categories are thoroughly discussed in the research paper.

This study has contributed to broaden our understanding of central factors affecting Norwegian companies' collaboration with the police on cybercrime, which in turn can contribute to improve the collaboration itself. Through my analysis and discussion, I have revealed correlations between existing literature and my empirical findings pointing out that the maturity of Norwegian companies related to digital security is based on awareness, risk perception, security culture, management, and level of preparedness. Likewise, the maturity of the police related to preventing and handling cybercrime is based on management's priorities, capacity, competence, external communication, visibility, structure, and organization. The work conducted on cybercrime within Norwegian companies and the Norwegian police have mutual influence on each other and make up the foundation of collaboration between private sectors and public authorities. Private sectors require the police to improve their work with cybercrime through the above-mentioned factors. This will motivate Norwegian companies to increase their degree of information sharing and involvement of the police regarding cybercrime. The police, on the other hand, is dependent on information from the companies in order to gain knowledge that will both contribute to a more targeted effort and also monitor trends and vulnerabilities exploited be cybercriminals. Central principles in this collaboration are trust, transparency, and mutual effort.

Conclusively, collaboration between Norwegian companies and the police regarding cybercrime relies on the companies' continuous work within security and preparedness and the ability of the police to build competence and capacity on the matter.

Sammendrag

Digitaliseringen av samfunnet fører med seg mange nye muligheter og fordeler som vi alle nyter godt av, samtidig som det også skaper nye sårbarheter som kriminelle og andre ondsinnede aktører utnytter. Norske virksomheter opplever daglig å bli utsatt for mindre alvorlig datakriminalitet, og flere virksomheter har også de siste årene blitt utsatt for alvorlig datakriminalitet som for eksempel dataangrep med påfølgende kryptering og løsepengekrav. Dette stiller nye krav til hvordan de norske virksomhetene jobber med sikkerhet og beredskap, og det utfordrer politiets evne til å løse sine oppgaver knyttet til forebygging, avverging, håndtering og etterforskning av datakriminalitet. Gjennom denne oppgaven har jeg tatt utgangspunkt i de menneskelige og organisatoriske faktorene som spiller inn på de norske virksomhetenes samarbeid med politiet, og jeg kom med det frem til følgende problemstilling: «*Hvilke faktorer påvirker norske virksomheters samarbeid med politiet når det kommer til forebygging og håndtering av datakriminalitet?*»

Litteraturen på området har jeg i all hovedsak hentet fra tradisjonelle teorier rundt menneskeskapte- og organisatoriske ulykker, høypålitelige organisasjoner og sikkerhetskultur. Samtidig har jeg også basert oppgaven på nyere forskning som tar for seg et privat-offentlig samarbeid, satt i en digital kontekst hvor datakriminalitet er en stor trussel for private virksomheter. I tillegg har jeg trukket inn offentlige dokumenter som plasserer politiet i dette landskapet og som tar for seg norske myndigheters tilnærming til digital sikkerhet.

Prosjektet ble gjennomført som en deskriptiv flercasestudie, med deltakelse fra to utvalg. Det ene utvalget representerer personer som sitter sentralt i norske virksomheter når det kommer til digitalt sikkerhetsarbeid og vurderingene rundt samarbeid med politiet, og det andre utvalget representerer personer som jobber med datakriminalitet og digital sikkerhet i politi- og lensmannsetaten, andre offentlige myndighetsorgan og private sikkerhetsselskaper. Datainnsamlingen ble gjennomført ved bruk av kvalitativ metode inspirert av grounded theory og SDI-modellen, og jeg gjennomførte totalt 18 dybdeintervjuer fordelt på de to intervjuutvalgene. Intervjuene ble transkribert, og videre kodet og kategorisert med bruk av analyseprogrammet NVivo. Etter en omfattende prosess med behandling av datamaterialet satt jeg igjen med et bredt datamateriale som dannet grunnlaget for fire hovedkategorier; «Politiets og datakriminalitet», «Virksomhetenes beredskapsarbeid», «Datakriminalitetens natur» og «Eksterne faktorer». Disse kategoriene har videre dannet grunnlaget for drøfting og konklusjon.

Studien har bidratt til verdifull innsikt i hvilke faktorer som påvirker norske virksomheters samarbeid med politiet, noe som kan danne et godt utgangspunkt for å bedre et privat-offentlig samarbeid når det kommer til forebygging og håndtering av datakriminalitet. Gjennom min analyse og drøfting har jeg funnet direkte sammenhenger mellom empirien og eksisterende litteratur, som blant annet viser at de norske virksomhetenes modenhet når det kommer til digital sikkerhet baserer seg på bevisstgjøring, risikoforståelse, sikkerhetskultur, og viktigheten av at sikkerhetsarbeidet forankres i ledelsen og at det gjøres gode forberedelser gjennom beredskapsarbeidet. På samme måte baserer politiets modenhet når det kommer til arbeid med datakriminalitet seg på prioritering fra ledelsen, kapasitet, kompetanse, kommunikasjon utad, synlighet, struktur og organisering. Arbeidet med digital sikkerhet og datakriminalitet hos de norske virksomhetene og politiets arbeid med datakriminalitet påvirker hverandre gjensidig og legger grunnlaget for samarbeidet. De norske virksomhetene ønsker at politiet skal ta mer eierskap til datakriminaliteten og øke sin kapasitet og kompetanse slik at virksomhetene i større grad opplever at det er et poeng å dele informasjon og involvere politiet når det kommer til både mindre alvorlig og alvorlig datakriminalitet. Politiet er avhengig av at virksomhetene deler informasjon slik at politiet kan målrette sin innsats og drive forebyggende arbeid basert på et kunnskapsgrunnlag om hva virksomhetene utsettes for, og hvordan trendene utvikler seg innen datakriminalitet. Sentrale prinsipper i dette samarbeidet er tillit, åpenhet og gjensidighet.

Min konklusjon ble at et godt samarbeid mellom norske virksomheter og politiet når det kommer til forebygging og håndtering av datakriminalitet bygger på hvordan norske virksomheter jobber med det digitale beredskapsarbeidet, og hvordan politiet bygger kapasitet og kompetanse for å møte kriminalitetsutfordringene knyttet til datakriminalitet. Verken de norske virksomhetene eller politiet kan møte utfordringene knyttet til datakriminalitet og trusler fra det digitale rom alene, og et samarbeid vil kunne være avgjørende for å opprettholde samfunnssikkerheten i fremtiden.

Forord

Denne masteroppgaven markerer avslutningen på mitt deltidsstudium Master i Beredskap og kriseledelse, ved Nord universitet. Oppgaven tar for seg samarbeidet mellom norske virksomheter og politiet når det kommer til forebygging og håndtering av datakriminalitet. Bakgrunnen for valg av tema var min interesse for sikkerhets- og beredskapsarbeid og viktigheten av samarbeid mellom private og offentlige aktører. De økende utfordringene knyttet til datakriminalitet og trusler fra det digitale rom gjorde at jeg ønsket å sette sikkerhet, beredskap og privat-offentlig samarbeid inn i en digital kontekst. Prosessen med oppgaven har vært interessant og lærerik fra start til slutt, og har gitt meg en dypere forståelse og innsikt i tematikken, noe som forhåpentligvis også kan komme andre til gode.

Jeg ønsker takke min veileder, Per Arne Godejord, for god veiledning gjennom tilgjengelighet og konstruktive tilbakemeldinger. Jeg vil også rette en stor takk til alle som stilte til intervju og bidro til et bredt og informasjonsrikt empirisk grunnlag. Deres villighet til å dele informasjon, erfaringer, refleksjoner og kunnskap har vært avgjørende for gjennomføringen av oppgaven. Videre vil jeg også takke både tidligere og nåværende arbeidsgiver som har lagt til rette slik at jeg har fått muligheten til å fullføre dette studieløpet. Gode venner er godt å ha, og jeg vil også takke venner som har delt erfaringer fra deres arbeid med masteroppgaver, gitt gode og konstruktive tilbakemeldinger og et objektivt blikk på oppgaven.

Å skrive en masteroppgave krever mye oppmerksomhet over en lengre periode, og det har til tider vært krevende å kombinere studier med fulltidsjobb og privatliv. Takket være en tålmodig og forståelsesfull samboer har jeg kommet i mål med oppgaven. Tusen takk, Gry!

Oslo, 25. mai 2022

Benedicte Bjartland

Innhold

Oversikt over tabeller og figurer

Tabelloversikt

Figuroversikt

Oversikt vedlegg

Begrepsordliste

NC3:	Nasjonalt cyberkrimsenter
NCSC:	Nasjonalt cybersikkerhetssenter
NSM:	Nasjonal sikkerhetsmyndighet
POD:	Politidirektoratet
IKT:	Informasjons- og kommunikasjonsteknologi
NorSIS:	Norsk senter for informasjonsforskning
Europol:	Europeisk organisasjon for politisamarbeid
NSR:	Næringslivets sikkerhetsråd
Sikkerhetsloven:	Lov om nasjonal sikkerhet, av 01.01.2019

1 Innledning

Norge er blant de fremste landene i verden til å ta i bruk ny teknologi. Digitale infrastrukturer og systemer blir stadig mer komplekse, omfattende og integrerte. Det skapes avhengigheter på tvers av ansvarsområder, sektorer og nasjoner, og det er en forventning om at digitale tjenester skal være tilgjengelige til enhver tid. Digitaliseringen av samfunnet byr på utfordringer gjennom nye sårbarheter, og en vellykket digitalisering handler like mye om at de nye løsningene må ivaretar krav til sikkerhet (Departementene, 2019).

De siste årene har utfordringene som digitaliseringen fører med seg fått mye fokus i arbeidet med samfunnssikkerheten. I strategien for å bekjempe IKT-kriminalitet beskriver Justis- og beredskapsdepartementet (2015) visjonen for det digitale rom. På lik linje med andre områder skal Norge være trygt og sikkert, gjennom å være rustet til å håndtere fremtidige kriser. Myndighetene og andre samfunnsaktører, og samspillet mellom dem, skal skape trygghet, forebygge, avverge, oppklare og straffeforfølge datakriminalitet. Når en borger, virksomhet eller viktig samfunnsfunksjon blir utsatt for datakriminalitet, skal politiet ha særlig oppmerksomhet på den som er rammet, forhindre skade, etterforske og iverksette straffeforfølgning for å ivareta deres rettssikkerhet og trygghet. Målet er å styrke samfunnssikkerheten og beredskapen (Justis- og beredskapsdepartementet, 2015).

Bare det siste året har flere norske virksomheter blitt utsatt for alvorlig datakriminalitet som har truet virksomhetenes eksistens, og satt både virksomhetene selv, samfunnet og private og offentlige aktører på prøve. Kriminelle, og andre ondsinnede aktører, utnytter i økende grad de sårbarhetene som følger med den digitale utviklingen. I arbeidet med dette er aktørene, både de offentlige og private, avhengige av å stå sammen. Et komplekst trussel- og risikobilde vil kreve en mer kompleks innsats. Med min egen bakgrunn fra en nødetat og andre arbeidsforhold med samfunnssikkerhet som fokus, kombinert med flere års studier innen beredskap og kriseledelse, har jeg fått stor interesse for utfordringene knyttet til datakriminalitet. Jeg har gjort meg noen antakelser om at det er et stort fokus på og ønske om samarbeid hos de forskjellige private og offentlige aktørene, samtidig som det også eksisterer utfordringer når det kommer til dette samarbeidet. Med bakgrunn i dette ønsket jeg å se nærmere på hva som påvirker samarbeidet mellom norske virksomheter og politiet i møtet med trusselen som datakriminalitet utgjør.

1.1 Aktualisering

Næringslivets sikkerhetsråd (NSR) har over tid sett at mange virksomheter ikke anmelder datakriminalitet, noe som knyttes til at de ikke har tillitt til politiets kompetanse eller kapasitet til å håndtere det. NSR mener at dette er en skummel utvikling og at det vil bli viktig at politiet får tilført ressurser for å snu trenden (NSR, 2021). Trusselen fra datakriminelle øker stadig og de kriminelle aktørene har blitt profesjonelle og sofistikerte i sine fremgangsmåter. De samarbeider, velger ut sine mål på en kalkulert måte og de beskrives som hensynsløse og metodiske i sin tilnærming. Utviklingen innen datakriminalitet går i en rasende fart og man ser at de kriminelle er svært tilpasningsdyktige. En økt innsats fra politiet internasjonalt de siste årene har ført til at de kriminelle utvikler metoder for å kunne operere sikkert. De utnytter også svakheter i politiets arbeid med datakriminalitet gjennom å for eksempel å utnytte det grenseoverskridende og globale elementet i datakriminalitetens natur for å vanskeliggjøre koordinering og samarbeid for politiet i forskjellige land. Utviklingen innen krypteringsteknologi og kryptovaluta gjør det også vanskelig å kunne spore de kriminelle gjennom deres kommunikasjon og pengespor. Sosial manipulering blir brukt aktivt i cyberoperasjonene for å omgå sikkerhetsteknologi og sikkerhetstiltak. Både kunnskapen og teknologien som de kriminelle benytter i forbindelse med sosial manipulering har blitt svært god (Europol, 2021). Disse momentene er i tråd med det norsk politi også beskriver som utfordringer knyttet til datakriminaliteten (POD, 2017).

Datakriminalitet begås først og fremst for økonomisk vinning, men i noen tilfeller er motivet å skade maskinvare eller digitale tjenester for å skaffe sensitiv informasjon. Datakriminaliteten rammer næringslivet, offentlige virksomheter, kritiske samfunnsfunksjoner og privatpersoner. Løsepengevirus har kostet næringslivet flere hundre millioner kroner de siste to årene. Et kjent eksempel er datainnbruddet mot Norsk Hydro i 2019 som kostet virksomheten ca. 600 millioner kroner. Selv om få datainnbrudd er vellykkede, er det stort potensial for profitt og mulighetene for å identifisere og straffeforfølge gjerningspersonene er små (POD, 2021).

Alle virksomheter har ansvar for å ivareta egen digital sikkert. Likevel kan verken myndigheter, virksomheter eller borgere håndtere de digitale utfordringene alene. Flere og flere virksomheter erkjenner at cyberoperasjoner kan ramme alle og Nasjonalt cybersikkerhetssenter (NCSC) erfarer at stadig flere prioriterer det digitale sikkerhetsarbeidet. Likevel er det fremdeles mange norske virksomheter som ikke har et forsvarlig sikkerhetsnivå (NSM, 2021). I stortingsmeldingen *IKT-sikkerhet – et felles ansvar* (2016-2017) trekkes det

frem at et styrket samarbeid mellom myndighetene og privat sektor vil kunne bidra til bedre situasjonsforståelse, beslutninger og bedre tilgang til ressurser (Meld. St. 38 (2016-2017).

For å kunne forebygge trenger man kunnskap. Rapportering, anmeldelser og åpenhet om kriminelle hendelser vil bidra til kunnskap om kriminalitet i et samfunn. I Mørketallsundersøkelsen (2020) kom det frem at en tredjedel av norske virksomheter ble utsatt for en uønsket digital sikkerhetshendelse i 2019, og av disse var det kun 11% av virksomhetene som rapporterte hendelsen til politiet (NSR, 2020). Det er ikke bare NSR som påpeker store mørketall når det kommer til datakriminalitet. I perioden 2013-2018 var det en reduksjon i anmeldelser på 30% i Oslo politidistrikt, noe som ses i sammenheng med at kriminaliteten har blitt mer digitalisert. Nedgangen av anmeldelser har vært spesielt merkbar når det kommer til vinningskriminalitet og mer tradisjonelle, «analoge» deler av kriminaliteten. Dette betyr ikke at det er mindre kriminalitet enn før, men det er vanskelig å si noe om kriminalitetsutviklingen fordi den ikke er kjent (Oslo politidistrikt, 2018). Lignende trender finner man også i England, USA, Canada og Nederland hvor det trekkes frem at det er stor underrapportering når det kommer til datakriminalitet rettet mot virksomheter, noe som vanskeliggjør det forebyggende arbeidet (Kemp, Buil-Gil, Miró-Llinares & Lord, 2021; Wanamaker, 2019; Van de Weijer, Leukfeldt & Van der Zee, 2019).

I den årlige rapporten *Nasjonalt digitalt risikobilde* trekker Nasjonal sikkerhetsmyndighet (NSM) frem åpenhet og deling av informasjon om uønskede digitale hendelser som viktig i arbeidet med å forebygge og håndtere datakriminalitet. Rapporten skal øke bevissthet og motivere til bedre digital sikkerhet i offentlige og private virksomheter. Åpenhet om for eksempel et dataangrep vil kunne bidra til økt risikoforståelse og sikkerhetsbevissthet hos virksomhetene og i samfunnet ellers, belyse viktigheten av behovet for god sikkerhet, vise at alle virksomheter, både offentlige og private, vil kunne bli utsatt for datakriminalitet og med det bidra til å etablere en åpenhetskultur. I tillegg til å være åpne og dele informasjonen med samfunnet er det viktig at informasjon om hendelsen deles med NSM, politiet og andre myndigheter (NSM, 2021).

Det finnes mange mulige forklaringer når det kommer til store mørketall innen datakriminalitet. Årsakene kan blant annet være at kriminaliteten ikke oppdages av den som har blitt utsatt for den, at tilliten til politiet er lav på dette kriminalitetsområdet eller at en virksomhet for eksempel er redd for sitt omdømme (Oslo politidistrikt, 2018). For at politiet skal få et bedre kunnskapsgrunnlag og være i stand til å målrette sin innsats, er det viktig at datakriminalitet blir anmeldt på lik linje med annen type kriminalitet. Selv om en sak blir

henlagt på grunn av manglende bevis kan det være informasjon om modus og øvrige spor som kan bidra til å styrke politiets kunnskapsgrunnlag, herunder styrke politiets evne til å forebygge og etterforske datakriminalitet (POD, 2017).

Det moderne samfunnet er i stor grad avhengig av IKT for å fungere. Det eksisterer imidlertid en systematisk forsinkelse mellom teknologiutvikling, metodeutvikling og organisasjonsutvikling. Det betyr at utfordringene som samfunnet står ovenfor, ikke minst trussel-, kriminalitets- og sårbarhets-bildet, utvikler seg raskere enn myndighetene hittil har klart å respondere (Justis- og beredskapsdepartementet, 2015). Forebygging er politiets hovedstrategi. I dette ligger det at politiet skal ha en systematisk, planmessig og kunnskapsbasert tilnærming til forebygging og samarbeide på tvers av fagområder og sektorer. Forebyggende innsats kan skje både før, under og i etterkant av en kriminell handling eller uønsket hendelse (POD, 2020). I en situasjon hvor bruk av ny teknologi utvikles raskt, er det utfordrende for politiet å bekjempe datakriminalitet. Trusselbildet krever at kunnskapsgrunnlaget for bekjempelse av kriminaliteten utvides og stiller nye krav til moderne IKT-utstyr og teknologisk kompetanse i politiet. Videre blir det større behov for samarbeid mellom politiet og andre aktører. Det er viktig at befolkningen har tillit til at alle typer kriminalitet bekjempes effektivt og godt (Departementene, 2019, s. 21).

Datakriminalitet håndteres av politidistriktene og av særorgan som Kripos og Økokrim. I riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT (2020-2021) kommer det frem klare svakheter som samlet sett vurderes som alvorlige. Dette dreier seg blant annet om manglende kompetanse og kapasitet innenfor etterforskning av datakriminalitet. Politiet mangler oversikt over datakriminalitet og prioriterer denne kriminalitetsformen i liten grad. Riksrevisjonen påpeker at manglende kompetanse og kapasitet kan utgjøre et rettssikkerhetsproblem ved at saker henlegges uten etterforskning, eller ved at de blir feilbehandlet. Uten nødvendig kompetanse til å bekjempe datakriminalitet kan også politiet miste tillit i befolkningen og i offentlige og private virksomheter. Blant de viktigste tiltakene som har blitt gjort i politiet i forbindelse med datakriminalitet er etableringen av enheter for digitalt politiarbeid (DPA) i alle politidistrikter i forbindelse med politireformen i 2015 og etableringen av Nasjonalt cyberkrimsenter (NC3) i Kripos i januar 2019. NC3 skal bistå distriktene og etterforske noen særlig alvorlige saker selv. I 2021 hadde NC3 kapasitet til å etterforske en–to større saker i året, noe som vil si at etterforskningen av datakriminalitetssakene i all hovedsak må skje i distriktene. Konsekvensene av lav kapasitet i DPA og NC3 er at teknologikrevende datakriminalitet henlegges. Sakene blir for store,

komplekse og ressurskrevende å etterforske for politidistriktene. At det ikke er gjort mer for å omstille politiet og sikre tilstrekkelig kompetanse og kapasitet til å håndtere et kriminalitetsbilde med stadig større innslag av datakriminalitet omtales som sterkt kritikkverdig av Riksrevisjonen (Riksrevisjonen, 2021).

Situasjonen vi i dag står overfor når det kommer til trusselen som datakriminalitet utgjør mot norske virksomheter er kompleks og utvikler seg raskt. Det er både private og offentlige aktører som jobber med forebygging og håndtering av uønskede digitale hendelser og datakriminalitet, og de norske virksomhetene har også selv et ansvar i dette. Politiets mandat når det kommer til datakriminalitet er å forebygge, avdekke, etterforske og straffeforfølge kriminalitet både i det fysiske og det digitale rom. Dette er oppgaver som til dels vil overlappe med mandatet til andre offentlige aktører, som for eksempel NSM. For at politiet skal kunne målrette sin innsats krever det en kunnskap om datakriminaliteten. For å kunne forebygge datakriminalitet rettet mot virksomheter og hjelpe virksomheter som har blitt utsatt for datakriminalitet må politiet få informasjon. I en Riksrevisjonens undersøkelse av politiets innsats mot datakriminalitet i 2021 kom det frem at politiet har klare svakheter når det kommer til arbeidet med datakriminalitet. I tillegg er mørketallene store når det kommer til rapportering og anmeldelser av datakriminalitet fra virksomhetene. Det finnes mange forsøk på å forklare hvorfor virksomheter ikke alltid rapporterer eller anmelder datakriminalitet til politiet. Et samarbeid mellom norske virksomheter og politiet omtales som sentralt i arbeidet med å forebygge og håndtere datakriminalitet i dag og for fremtiden. Denne oppgaven søker å belyse hva som påvirker dette samarbeidet. For å kunne legge til rette for og forbedre et viktig samarbeid må vi vite noe om hva årsakene er til at et slikt samarbeid er utfordrende.

1.2 Problemstilling og forskningsspørsmål

Med bakgrunn i min interesse for datakriminalitet og antakelser om at det finnes utfordringer når det kommer til samarbeidet mellom næringslivet og politiet når det kommer til dette temaet, utarbeidet jeg en problemstilling som kunne være med på å belyse bakenforliggende årsaker til hvorfor samarbeidet er som det er, for å kunne identifisere hva som kan gjøres for å bedre samarbeidet og med det stå sterkere sammen i kampen mot datakriminaliteten. På bakgrunn av dette kom jeg frem til problemstillingen:

Hvilke faktorer påvirker norske virksomheters samarbeid med politiet når det kommer til forebygging og håndtering av datakriminalitet?

For å besvare problemstillingen utarbeidet jeg følgende forskningsspørsmål:

- *Hvordan påvirker politiets arbeid med datakriminalitet virksomhetenes samarbeid med politiet?*
- *Hvordan påvirker virksomhetenes beredskapsarbeid samarbeidet med politiet?*
- *Hvilke faktorer spiller inn på virksomhetenes beslutning om å kontakte politiet dersom de blir utsatt for datakriminalitet?*
- *Hvilke forventninger har virksomhetene til politiet når det kommer til samarbeid og forebygging og håndtering av datakriminalitet?*
- *Hva kan politiet gjøre for å legge bedre til rette for et godt samarbeid med virksomhetene?*
- *Hvordan spiller samfunnet, media og datakriminalitetens natur inn på samarbeidet mellom politiet og virksomhetene?*

Jeg har ikke funnet og er ikke kjent med at det er gjennomført ligende forskningsprosjekter i Norge med den samme vinklingen på problematikken, men jeg har funnet ligende undersøkelser fra blant annet Canada, Nederland og England (Wanamaker, 2019; Van de Weijer et al., 2019; Kemp et al., 2021). Det eksisterer også norske undersøkelser gjenomført av både private og offentlige aktører som kan gi noe innsikt i tematikken. Jeg håper at oppgaven kan bidra til bedre forståelse for hva som påvirker samarbeidet mellom virksomhetene og politiet når det kommer til datakriminalitet, og at denne innsikten og kunnskapen kan bidra til at både virksomheter og politiet kan ta med seg nyttig informasjon videre i samarbeidet for forebygging og håndtering av datakrminalitet.

1.3 Operasjonalisering og avgrensning

Denne oppgaven er skrevet i et samfunnsvitenskapelig fag. Med bakgrunn i dette vil jeg fokusere på de menneskelige og organisatoriske forholdene knyttet til de norske virksomhetene og politiet i samarbeidet med håndtering og forebygging av datakriminalitet. Innenfor tematikken opptrer de tre elementene menneske, organisasjon og teknologi ofte sammen. Der teknologi blir trukket frem som tema og diskutert vil dette ikke være på et dypt teknologisk plan, men heller med fokus på generelle tilnærminger om for eksempel kostnader for sikkerhetsteknologi.

1.3.1 Samfunnssikkerhet og datakriminalitet

Begrepet sikkerhet brukes ofte om forebyggende tiltak som har til hensikt om å redusere sannsynligheten for at noe uønsket skal skje eller redusere konsekvensene av uønskede

hendelser. Sikkerhet brukes også om den evnen et system har til å unngå skader og tap. Sikkerhet kan relateres til det fysiske miljøet, som teknologiske systemer, produkter og omgivelsene generelt, og til menneskelige og sosiale faktorer som dreier seg om atferd, organisasjonskultur, politikk, beslutninger og lignende. Sikkerhet kan også knyttes til forskjellige nivå som individ, organisasjon og samfunn, eller til ulike faser i en prosess (Aven, Boyesen, Njå, Olsen & Sandve, 2019, s. 17).

Samfunnssikkerhet er den evnen samfunnet har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påkjenninger (Meld. St. 17 (2001-2002). Beredskap og kriseledelse er begreper nært tilknyttet samfunnssikkerhet. Ofte trekkes store ulykker som Scandinavian star i 1990 og ulykken på oljeplattformen Alexander Kielland i 1980 frem i forbindelse med samfunnssikkerhet (Aven et al., 2019). Som samfunnet ellers har arbeidet med samfunnssikkerhet også blitt påvirket av digitaliseringen, gjennom å åpne opp for nye muligheter når det kommer til risikohåndtering, beredskap og kriseledelse, i tillegg til at digitaliseringen stadig fører til nye sårbarheter og risikoer (Engen, Pettersen Gould, Kruke, Hempel Lindøe, Olsen & Olsen, 2021, s. 245).

På norsk har vi kun ett ord for sikkerhet, mens på engelsk har man ordet safety, som omhandler risikoen og usikkerheten knyttet til ikke-planlagte handlinger og hendelser. Ordet security benyttes i forbindelse med usikkerheten og risikoen knyttet til tilsiktede uønskede handlinger som for eksempel kriminalitet, også kalt ondsinnede handlinger (Engen et al., 2021, s. 101). Samfunnssikkerhetsbegrepet er ment til å dekke et bredt spekter av utfordringer, og omfatter både ondsinnede handlinger, som for eksempel kriminalitet, og ikke intenderte hendelser som for eksempel en naturkatastrofe (Aven et al., 2019, s. 17). Uønskede hendelser er hendelser som forårsaker eller kunne ha forårsaket ulike typer skader på sentrale verdier. En uønsket hendelse kan være en ulykker, kriser og katastrofer, og man skiller gjerne mellom disse ved å se på størrelse eller omfang av hendelsen. En ulykke er gjerne en uønsket hendelse av mindre omfang som etablerte responsstrukturer lokalt kan håndtere. En krise har større omfang og krever en mer omfattende respons og mobilisering. En katastrofe er en hendelse som medfører store ødeleggelser og krever omfattende mobilisering av responskapasiteter nasjonalt og noen ganger internasjonalt (Engen et al., 2021, s. 302).

I denne oppgaven knyttes begrepene sikkerhet, samfunnssikkerhet og uønskede hendelser til ondsinnede handlinger i form av datakriminalitet. Datakriminalitet kan som kriminalitet ellers være mindre alvorlig eller alvorlig, og en slik hendelse trenger ikke

nødvendigvis å materialisere seg i en stor krise. Typiske eksempler på mindre alvorlig datakriminalitet er at man mottar en svindel e-post, som er noe som skjer hyppig og er godt kjent for mange virksomheter. Samtidig kan, dersom den kriminelle aktøren lykkes, den samme e-posten utløse en krise gjennom at mottakeren oppgir brukernavn og passord og den ondsinnede aktøren kan komme seg inn i virksomhetens systemer.

1.3.2 Digital sikkerhet og datakriminalitet – et hav av begreper

Både i litteraturen jeg har benyttet til oppgaven, i offentlige skriv fra forskjellige myndigheter og blant informantene ble det benyttet mange forskjellige begreper i forbindelse med sikkerhet på digital arena. Det har ikke vært vanskelig å forstå at det er den samme meningen som ligger bak de forskjellige begrepene, men det kan skape usikkerhet når forskjellige begreper benyttes om hverandre. For eksempel kan informasjonssikkerhet og cybersikkerhet betegne sikkerhet vedrørende informasjon, men både i det fysiske og i det digitale domenet.

Begrepene datasikkerhet, IKT-sikkerhet, informasjonssikkerhet, cybersikkerhet og digital sikkerhet, er begreper med delvis samme betydning. Datasikkerhet var populært på 1980-tallet, cybersikkerhet dukket opp på 2010-tallet, mens digital sikkerhet ble etablert av norske myndigheter i 2019 som et samlebegrep for begrepene nevnt her. Digital sikkerhet omhandler beskyttelse av digital informasjon (Jøsang, 2021, s. 13). Videre i oppgaven vil jeg forholde meg til begrepet digital sikkerhet da oppgaven sikter seg inn mot datakriminalitet som foregår på det digitale domenet og på den måten treffer digital informasjon. Likevel er det verdt å nevne at informasjonen som eksisterer digitalt også i noen tilfeller kan eksistere fysisk og bli utnyttet digitalt, for eksempel i forbindelse med sosial manipulasjon.

På lik linje som med digital sikkerhet opplevde jeg at det ble benyttet mange begreper om datakriminalitet. Dette kom frem både i intervjuene, i litteraturen og i offentlige dokumenter fra myndigheter og andre organisasjoner som publiserer informasjon om tematikken. Begrepene IKT-kriminalitet, datasikkerhetshendelser, cyberkriminalitet, informasjonssikkerhetshendelser, datainnbrudd og digitale angrep er blant begrepene som har kommet frem under studien. En datasikkerhetshendelse er et eksempel på et begrep som retter seg mot en uønsket hendelse som ikke faller innunder kriminalitetsbegrepet. Dette kan kanskje heller være en ikke ondsinnet uønsket hendelse i et teknologisk system. Utover dette er andre uønskede hendelser utført av en kriminell aktør å anse som kriminalitet. Med IKT-kriminalitet forstås kriminalitet som retter seg mot datasystemer og/eller datanettverk, eller kriminalitet der sentrale elementer av handlingsforløpet begås ved hjelp av datautstyr og/eller

datanettverk. Med IKT-hendelser forstås hendelser i det digitale rom hvor det kan oppstå negative samfunnsmessige konsekvenser. I motsetning til IKT-kriminalitet, trenger ikke hendelsene å være utløst av en kriminell handling eller unnlatelse. Likevel kan politiets oppmerksomhet være nødvendig på samme måte som under andre hendelser, eksempelvis større samfunnsmessige ulykker (Justis- og beredskapsdepartementet, 2015).

IKT-kriminalitet kan deles inn i to grupper; (1) kriminalitet rettet mot datasystemer og (2) bruk av IKT som sentralt verktøy i utøvelsen av annen kriminalitet (POD, 2017). Dette er i tråd med internasjonale begreper som cyber-dependent crime og cyber-facilitated crime (Europol, 2017). Selv om IKT-kriminalitet er det begrepet som hyppigst blir brukt i offentlige dokumenter fra blant andre Politidirektoratet og Justis- og beredskapsdepartementet vil jeg videre i oppgaven bruke begrepet datakriminalitet da dette er det begrepet politiet bruker som den operative betegnelsen på digital kriminalitet. Selv om løsepengevirus stadig trekkes frem som den mest alvorlige kriminaliteten som retter seg mot norske virksomheter, vil oppgaven ta for seg datakriminalitet som helhet, med både mindre alvorlig og alvorlig datakriminalitet. Det vil ikke være et spesifikt fokus på de forskjellige typene datakriminalitet. Datakriminalitet vil som både mindre alvorlige uønskede hendelser som inntreffer ofte, og større alvorlige uønskede hendelser som dataangrep og løsepengevirus, settes i en samfunnssikkerhetskontekst der dette er hendelser som truer norske virksomheter i dag og setter både offentlige og private aktører på prøve når det kommer til samarbeidet.

1.3.3 Politiet og de andre offentlige aktørene

Det er flere offentlige aktører som har en rolle i arbeidet med datakriminalitet, og noen av mandatene til disse aktørene vil i noen grad være overlappende. Årsaken til dette er at en uønsket digital hendelse vil kunne true for eksempel en samfunnskritisk funksjon som vil falle under NSM sitt mandat (DSB, 2016), samtidig som det også er datakriminalitet og vil falle innunder politiets mandat (POD, 2017; Departementene, 2019). Gjennom arbeidet med oppgaven har det kommet tydelig frem at det er en del usikkerhet når det kommer til hvilken offentlig myndighet som gjør hva i forbindelse med datakriminalitet. Dette gjelder spesielt forskjellen mellom arbeidet som politiet og NSM gjør knyttet til denne tematikken.

Politiet skal beskytte samfunnet og forebygge, avdekke, etterforske og straffeforfølge kriminalitet. Denne oppgaven er den samme i det digitale rom som i det fysiske rom (Departementene, 2019, s. 21). Datakriminalitet håndteres av politidistriktene og av særorgan som Kripos og Økokrim. I forbindelse med nærpolitireformen i 2015 ble det etablert enheter

for digitalt politiarbeid (DPA) i alle politidistrikter (Riksrevisjonen, 2021). Kripos er politiets nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet (Departementene, 2019). Nasjonalt cyberkrimsenter (NC3), som er en del av Kripos, skal utvikle politiets kapasitet og kompetanse for å møte et mer digitalisert kriminalitets- og trusselbilde. Hovedoppgaver er å bekjempe datakriminalitet gjennom etterretning, metodeutvikling, forebygging, etterforskning, sikring av digitale spor samt patruljering på nett. Senteret vil spille en viktig rolle i å fremme informasjonsdeling og samvirke mellom private og statlige sikkerhetsaktører nasjonalt og internasjonalt (Politiet, u.å.). Økokrim er spissorganet i politiet og påtalemyndigheten for bekjempelse av økonomisk kriminalitet og miljøkriminalitet. Mange bedrageri gjennomføres i dag ved bruk av internett, noe som har medført at bedrageri i større grad gjennomføres over landegrensene og dermed mellom ulike jurisdiksjoner. Med bakgrunn i dette samarbeider gjerne Økokrim og politiet ellers og Kripos når det kommer til datakriminalitet (Økokrim, u.å.).

NSM har ifølge sikkerhetsloven et sektorovergripende ansvar for forebyggende sikkerhetstjeneste (Justis- og beredskapsdepartementet, 2015). NSM er det nasjonale fagmiljøet for digital sikkerhet og er en nasjonal varslings- og koordineringsinstans for alvorlige dataangrep som rammer samfunnskritiske funksjoner og infrastruktur (Departementene, 2019). NCSC er en del av NSM og er en arena for nasjonalt og internasjonalt samarbeid innen deteksjon, håndtering, analyse og rådgivning knyttet til digital sikkerhet. Senteret omfatter partnere fra næringsliv, akademia, forsvar og offentlig sektor som bidrar aktivt inn i et gjensidig samarbeid for et sterkere digitalt Norge. (NSM, u.å.). Opprettelsen av NCSC og NC3 i Kripos illustrerer myndighetenes satsning på digital sikkerhet. NCSC og NC3 skal komplementere hverandre og bidra til å konsolidere og styrke den nasjonale innsatsen i det digitale domenet (NSM, 2020).

I denne oppgaven er det primært politiets arbeid med forebygging og håndtering av datakriminalitet som har fokus. Med forebygging menes den innsatsen og de tiltakene politiet setter i verk politiet for å redusere forekomsten av kriminelle handlinger og uønskede hendelser, redusere skadevirkningene og hindre gjentakelse (POD, 2020, s. 6). Med håndtering menes politiets jobb med å avdekke, etterforske og straffeforfølge kriminalitet, Politiets forebygging og håndtering av datakriminalitet gjelder på lik linje i det digitale rom som i det fysiske rom. (Departementene, 2019, s. 21). Forebygging og håndtering handler altså om politiets innsats for å forhindre at norske virksomheter blir utsatt for datakriminalitet, i tillegg til å håndtere datakriminaliteten dersom den skjer. Dette kan handle om alt fra å

hjelpe virksomhetene i deres beredskapsarbeid for at de skal kunne sikre seg selv, til å gi beslutningsstøtte i en kaotisk situasjon dersom de har blitt utsatt for alvorlig datakriminalitet.

1.4 Oppgangens oppbygging

Kapittel 1 har gitt en innføring i og aktualisering av tematikken for oppgaven. Videre har problemstillingen og forskningsspørsmålene blitt presentert, og jeg har operasjonalisert begreper og avgrenset oppgaven. Videre vil kapittel 2 presentere sentral internasjonal teori og litteratur innen samfunnssikkerhet og beredskap. Dette er i all hovedsak teoriene om menneskeskapte ulykker, organisatoriske ulykker og høypålitelige organisasjoner. I tillegg presenteres sentral litteratur som treffer tematikken i norske forhold og som viser politiets rolle når det kommer til forebygging og håndtering av datakriminalitet. Dette danner oppgavens teoretiske rammeverk. I kapittel 3 presenteres metodiske momenter. Her beskrives valgene jeg har tatt når det kommer til forskningsdesign og metode for gjennomføring av studien og besvarelse av problemstillingen. Resultatene fra datainnsamlingen presenteres i kapittel 4 hvor funnene fra studien blir presentert i tre hovedkategorier med bruk av utdrag fra intervjuene. De tre hovedkategoriene er «Politiets og datakriminalitet», «Virksomhetenes beredskapsarbeid» og «Datakriminalitet, media og samfunnet». Funnene fra intervjuene som blir presentert i kapittel 4 vil videre bli drøftet opp mot kjerneelementene fra det teoretiske rammeverket i kapittel 5 under de fire områdene «Bevissthet», «Beredskapsarbeid», «Samvirke» og «Modenhet», som baserer seg på de empiriske funnene og kjerneelementene fra det teoretiske rammeverket. Til slutt blir konklusjonene presentert i kapittel 6 sammen med refleksjon rundt muligheten for videre forskning.

2 Teori

I dette kapitlet vil jeg gjøre rede for deler av teorien som er relevant for oppgavens problemstilling. Dette danner det teoretiske rammeverket og har til hensikt å skape utgangspunktet for den videre drøftingen av funnene i oppgavens analysekapittel. Hovedfokuset i dette kapitlet er teoriene om menneskeskapte- og organisatoriske ulykker og høypålitelige organisasjoner. Dette er kjente og sentrale internasjonale teorier innen fagfeltet. I tillegg vil jeg belyse sentral litteratur som knytter seg til samfunnssikkerhet og beredskap i en norsk kontekst og politiets rolle når det kommer til forebygging og håndtering av datakriminalitet. Innledningsvis vil jeg forankre oppgavens tematikk og problemstilling innenfor fagfeltets begrepsmessige rammer.

2.1 Risiko, risikosamfunnet og risikoforståelse

En velkjent definisjon er at risiko er produktet av sannsynlighet og konsekvens. Det er likevel ikke enkelt å «beregne» risiko, spesielt ikke når det kommer til risikoene knyttet til vårt digitaliserte samfunn (Engen et al., 2021, s. 92). Aven og Renn (2010) ser på risikobegrepet som usikkerhet utover en tallfestet sannsynlighet, basert på usikkerheten om og alvorligheten av uønskede hendelser og konsekvenser av en aktivitet med hensyn til det mennesker verdsetter (Aven & Renn, 2010, referert i Engen et al., 2021, s. 94). Risiko kan også uttrykkes som forholdet mellom trusselen mot en gitt verdi og verdiens sårbarhet mot denne trusselen. Sårbarheten må også ses i sammenheng med evnen til å motstå og forsvare seg mot trusler (Engen et al., 2021, s. 101). I et konstruktivistisk kunnskapssyn og gjennom de samfunnsvitenskapelige synene på risiko handler risiko om hvordan vi som individer og kollektiv forstår og tolker risiko, og risiko blir noe vi mennesker konstruerer. Risikoforståelse omhandler hvordan vi oppfatter og håndterer risiko. Risiko er noe vi må forholde oss til på alle samfunnsnivåer og i samspillet mellom enkeltindivider, virksomheter og organisasjoner og institusjoner (Engen et al., 2021, s. 92; Aven et al., 2019, s. 40).

Aven et al. (2019, s. 21) og Engen et al. (2021, s. 128) viser til den tyske sosiologen Ulrich Beck (1992) skriver om dagens risikosamfunn, et samfunn som er preget av digitaliseringen. Denne utviklingen har koplet det nasjonale og internasjonale samfunnet tettere sammen noe som effektiviserer viktige prosesser, som for eksempel raskere informasjons- og beslutningsprosesser. Risikosamfunnet kjennetegnes av samspillet mellom komplisert teknologi, komplekse organisasjoner og individuell handling i omgivelser som stadig er i endring (Aven et al., 2019, s. 21-22; Engen et al., 2021, s. 128-129). I et utvalg

opprettet i 1999 ble samfunnets sårbarhet og beredskap vurdert. Utvalget pekte på flere sikkerhetsutfordringer, blant annet et åpnere verdenssamfunn, teknologiske endringer som gir mer komplekse teknologiske systemer, økende kostnads- og effektivitetspress i næringslivet som skaper et næringsliv i stadig omstilling, og den økende kompleksiteten ved for eksempel avhengigheten av elektroniske informasjons- og kommunikasjonssystemer (NOU 2000:24; Aven et al., 2019, s. 22). Spesialiseringen i arbeidslivet har skapt større avhengighet mellom virksomheter og mellom ulike geografiske områder. Hele vår produksjon og virke er basert på stabil energitilførsel og tilgang på informasjons- og kommunikasjonstjenester. Disse kompliserte og tette koplingene har gitt oss gevinster i form av økt effektivitet og produktivitet, men samtidig økt sårbarhet. Når først noe går galt kan konsekvensene bli omfattende (Aven et al., 2019, s. 21; Bergsjø & Windvik, 2018, s. 17).

2.2 Forebygging, beredskap, kriser og samarbeid

Proaktivt sikkerhetsarbeid for å forebygge ulykker har høy prioritet i arbeidet med samfunnssikkerhet. Forebygging betyr konstant jobbing med en dynamisk ikke-hendelse (Weick, 1987, referert i Engen et al., 2021, s. 299). Målet er at uønskede hendelser ikke skal skje, men vi kan imidlertid ikke forebygge alle uønskede hendelser (Boin mfl., 2005, referert i Engen et al., s. 299). Forebygging er politiets hovedstrategi og er i kjernen av politiets samfunnsoppdrag. Forebygging omfatter arbeidet som politiet utfører alene og sammen med andre for å redusere forekomsten av kriminelle handlinger og uønskede hendelser. Samfunnssikkerhet og beredskap er sentrale deler av politiets forebyggende innsats. I strategien ligger det at politiet skal være i forkant av kriminaliteten, noe som baserer seg på en systematisk, planmessig og kunnskapsbasert tilnærming til forebygging og samarbeide på tvers av sektorer og fagområder. Forebygging skal skje både før, under og etter en kriminell handling eller uønsket hendelse (POD, 2020, s. 8-9). Politiet skal beskytte samfunnet og forebygge, avdekke, etterforske og straffeforfølge kriminalitet, og disse oppgavene skal være de samme i det digitale rom som i det fysiske rom (Departementene, 2019, s. 21).

Kriser kan fremstå tilsynelatende helt uventet (Turner, 1976, referert i Engen et al., 2021, s. 299), men de kan også være hendelser vi burde ha sett komme (Prince, 1920, referert i Engen et al., 2021, s. 299). Det finnes mange definisjoner på hva en krise er, noe er i tråd med et økende antall «nye kriser» knyttet til risikosamfunnet. Det er likevel noen sentrale elementer i krisebegrepet som går igjen, til tross for de mange definisjonene; usikkerhet, tidspress, trussel, tap, forstyrrelser av en normaltilstand, forhindring av normale og viktige

funksjoner, håndtering og beslutninger (Engen et al., 2021, s. 300). Sårbarhetsutvalget definerer en krise som en hendelse som har et potensial til å true viktige verdier og svekke en virksomhets evne til å utføre sine samfunnsfunksjoner (NOU 2000:24). I følge Quarantelli (2000) er ulykker, kriser og katastrofer alle uønskede hendelser med noen sentrale fellestrekk. Man skiller gjerne mellom dem ved å se på størrelse, omfang og ressursene som trengs for å håndtere hendelsen (Quarantelli, 2000, referert i Engen et al., 2021, s. 302). Det er vanlig å dele inn en krise i tre faser; førkrisefase, akutt krisefase og etterkrisefase (Kruke 2012, 2020; Olson 2000; Turner 1976, referert i Engen et al., 2021, s. 304). Det finnes også forskjellige typer kriser, som grovt kan deles inn i ondsinnede handlinger og utilsiktede hendelser. Et eksempel på en utilsiktet hendelse er en naturkatastrofe. Ondsinnede handlinger er hendelser iverksatt av mennesker som har en intensjon om å iverksette dem. Dette kan for eksempel være sabotasje, terror og kriminalitet (Engen et al., 2021, s. 312). Oppgavens dreier seg i all hovedsak om alvorlig datakriminalitet som kan utløse en krise hos norske virksomheter og i samfunnet, men også mindre alvorlig datakriminalitet som norske virksomheter utsettes for daglig. I tillegg vil oppgaven rette seg mot samarbeidet mellom norske virksomheter og politiet i krisens førkrisefase, akutte krisefase og etterkrisefase.

Beredskap er tiltak for å forebygge, begrense eller håndtere uønskede ekstraordinære hendelser (NOU 2000:24; Lunde, 2014, s. 43). Hensikten med beredskapsarbeidet er å forutse mulige trusler og utfordringer slik at de kan håndteres på en effektiv måte, for så å etablere kapasiteter for å håndtere dem. Beredskap kan på ses på som både et produkt, en aktivitet, en tilstand og en dynamisk og kontinuerlig prosess. Som produkt er beredskap gjerne en beredskapsplan som baserer seg på aktiviteter som risiko- og sårbarhetsanalyser, trening og øving. Beredskap er også en tilstand som sier noe om hvor forberedt og klar man er for å håndtere uønskede hendelser. Beredskap omfatter både det individuelle, organisatoriske og samfunnsnivået (Engen et al., 2021, s. 321). Beredskapsarbeidet til norske virksomheter vil i dag bestå av både fysisk og digital beredskaps om skaper en helhet.

Sentralt i arbeidet med samfunnssikkerhet er styring og planlegging i forebyggende øyemed. Det vil imidlertid alltid eksistere en restrisiko, og hendelser som oppstår til tross for det forebyggende arbeidet må håndteres på en effektiv måte ved hjelp av de samlede tilgjengelige ressursene, basert på klare strukturer, ansvarsforhold og kommandolinjer mellom de ulike involverte aktørene. Kvaliteten på håndteringen av en krise i den akutte fasen vil avhenge av hva som er gjort av forebygging og forberedelse i førkrisefasen, og læring i etterkrisefasen (Engen et al., 2021, s. 320). Begrepet samstyring er en ikke-hierarkisk prosess

der offentlige og private aktører og ressurser koordineres for å drive risikostyring, beredskapsarbeid og hendelseshåndtering (Røiseland & Vabo, 2012, referert i Engen et al., 2021, s. 213). I risikosamfunnet vil det være behov tett samarbeid mellom offentlige og private aktører for å møte et komplekst trussel- og risikobilde.

Siden ingen sektor i det norske samfunnet kan håndtere store uønskede hendelser, digitale som fysiske, alene er samfunnssikkerheten tuftet på et omfattende samvirke og samarbeid i førkrisefasen og i den akutte krisefasen. Man kan også se elementer av samarbeid i etterkrisefasen når det for eksempel kommer til læring og evaluering. Vi har fire samfunnssikkerhets- og beredskapsprinsipper *(1) Ansvarsprinsippet* går ut på at den myndigheten, virksomheten eller etaten som til daglig har ansvar for et område, har også ansvaret for nødvendige beredskapsforberedelser og for å utøve den tjenesten ved kriser og katastrofer, *(2) Likhetsprinsippet* handler om at den organiseringen man opptrer med under kriser, skal være mest mulig lik den organiseringen man har til daglig. Dette blir på mange måter en forlengelse av ansvarsprinsippet gjennom en understreking av at ansvarsforholdene internt i og mellom virksomheter ikke skal endres i forbindelse med krisehåndtering, *(3) Nærhetsprinsippet* sier at krisen skal håndteres på lavest mulig nivå. Det vil si at den som har størst nærhet til krisen, vanligvis vil være den som har best forutsetning for å forstå situasjonen, og dermed er best egnet til å håndtere den, *(4) Samvirkeprinsippet* sier at myndighet, virksomhet eller etat har et selvstendig ansvar for å sikre best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering (Engen et al., 2021, s. 324-325; Aven et al., 2019, s. 28).

Blant de overordnede målene i nasjonal strategi for digital sikkerhet finner vi målet om at norske virksomheter digitaliserer på en sikker og tillitsvekkende måte og har bedre evne til egenbeskyttelse mot datakriminalitet og uønskede digitale hendelser. Et annet overordnet mål er at politiet skal styrke sin evne til å bekjempe datakriminalitet. De styrende prinsippene som gjelder disse målene, omhandler samarbeid mellom næringslivet og myndighetene. Samarbeidet skal blant annet føre til å identifisere, utveksle erfaringer og drøfte digitale sikkerhetsutfordringer, det skal være forpliktende for begge parter og være basert på åpenhet, tillit og gjensidighet (Departementene, 2019, s.7-9).

2.3 Sikkerhetskultur - Mennesker, teknologi og organisasjon

I samfunnsvitenskapen definerer man kultur som et fellesskap av ideer, verdier og normer som en gruppe mennesker deler (Bergsjø, Windvik & Øverlier, 2020, s. 34).

Organisasjonskultur kan ikke reduseres til observerbar atferd og individuelle opplevelser, det omhandler et komplekst system av symboler og meninger, bestående av historier, ritualer og andre verdimessige uttrykk som gjennomsyrer sikkerheten i en organisasjon (Turner & Pidgeon 1997; Richter & Koch, 2004; Antonsen, 2009, referert i Engen et al., 2021, s. 175).

Sikkerhetskultur i en virksomhet handler om hvilke særtrekk som i større eller mindre grad bidrar til fokus på sikkerhet. Verdier, forståelse av hvordan oppgaver skal utføres, organisasjonsstruktur, sanksjoneringsmekanismer og normer for atferd er slike særtrekk. Sikkerhetskulturen handler om den kollektive forståelsen av *hva* som er farlig og *hvordan* man kan bidra til å redusere farene. En virksomhets sikkerhetskultur vil også kunne spille inn på beredskapsarbeidet og sikkerhetstiltakene ved at sikkerhetskulturen vil kunne være avgjørende når det kommer til det å ta snarveier og enkle løsninger på bekostningen av målene for sikkerhet (Aven et al., 2019, s. 34).

I 2016 ble begrepet digital sikkerhetskultur for første gang beskrevet og kartlagt i Norge (NorSIS, 2016). Tradisjonelt har både sikkerhetskultur og digital sikkerhetskultur blitt regnet som en del av organisasjonskulturen, altså felles utførelse av handlinger og oppgaver i en virksomhet. Som et resultat av dette har digital sikkerhetskultur blitt sett på som et verktøy for effektiv etterlevelse av regler og krav. Det finnes i dag flere definisjoner på digital sikkerhetskultur. De fleste definisjonene omfatter noen sentrale elementer; beskyttelse av digitale verdier fra ulike former for trusler som rettes mot innebygde sårbarheter. Den definisjonen jeg velger å forholde meg til er digital sikkerhetskultur kan forstås som de verdier, holdninger, antakelser, normer og kunnskaper som mennesker bruker når de forholder seg til digitale verdier (Bergsjø et al., 2020, s. 36). Ofte når det er snakk om digital sikkerhetskultur og atferd fokuseres det på enkeltindividet. Dersom vi skal knytte digital sikkerhetskultur til organisasjoner og virksomheter settes begrepet digital sikkerhetskultur inn i et mer kollektivt perspektiv. Dette handler for det første om hvilken digital sikkerhetskultur som eksisterer i en virksomhet og hvorvidt enkeltindivider og virksomheten som et kollektiv forholder seg til sikkerhet (Bergsjø et al., 2020, s. 37). Norsk senter for informasjonsforskning (NorSIS) trekker frem åtte kjerneområder som beskriver digital sikkerhetskultur på en helhetlig måte; (1) Fellesskap, (2) Styring og kontroll, (3) Tillit, (4) Risikooppfattelse, (5) Optimisme for teknologi og digitalisering, (5) Kompetanse, (7) Interesse for teknologi og IT, (8) Adferdsmønstre (NorSIS, 2016, referert i Bergsjø et al., 2020, s. 36).

Som tidligere nevnt er verdier, trusler og sårbarheter sentrale begreper innen risiko. I risikosamfunnet er risikobildet i stadig endring. Flere og flere verdier «kobles til nett» og

inngår på den måten i digitaliseringen. Dette gir nye former for sårbarheter og trusler, og med det nye former for risiko (Aven et al., 2019, s. 21; Engen et al., 2021, s. 128; Bergsjø et al., 2020, s. 20). Man kan dele sårbarheter og tilhørende sikringstiltak inn i tre kategorier; mennesker, teknologi og organisasjon. De tre kategoriene viser hvordan menneskene som jobber i en virksomhet, teknologien virksomheten benytter seg av og hvordan virksomheten er organisert med tanke på ansvar, ledelse, anskaffelser og personvern, alle spiller inn på hvordan virksomheten må se på sårbarheter og beredskapsarbeid for å sikre virksomheten (NSM, 2016, referert i Bergsjø et al., 2020, s. 20-21). Nätt og Heide (2019) trekker frem viktigheten av menneskenes kunnskap om datasikkerhet og hvilke sårbarheter som knyttes både til teknologien og våre svakheter som mennesker er essensielt for å opprettholde sikkerhet. Det er også viktig med sikkerhet gjennom teknologiske løsninger, men dette alene vil ikke kunne hindre ondsinnede aktører. I tillegg hjelper det ikke om bare enkeltpersoner i en virksomhet er opptatt av sikkerhet. Dette krever fokus på og arbeid med sikkerhet (Nätt & Heide, 2019, s. 25). Tekniske sikkerhetstiltak alene vil ikke stoppe trusselaktører, det er nødvendig med gode prosesser i virksomheten og god sikkerhetskultur hos brukere av systemer og virksomhetens ansatte. Dette øker robusthet, men også bevissthet og forståelse for sikkerhet hos den enkelte (NSM, 2021). Digital sikkerhetskultur i en virksomhet vil, i tråd med de åtte kjerneområdene til NorSIS som vist over, kunne fange opp de menneskelige, teknologiske og organisatoriske elementene i arbeidet med digital sikkerhet i en virksomhet.

2.4 Beredskapsteorier

Det finnes flere teorier som er utviklet i forlengelsen av ulykker og katastrofer. Teoriene gir grunnlag for større forståelse av organisatoriske sårbarheter og kunnskap som kan lede fram til bedre styring av pålitelighet og sikkerhet i organisasjoner, samt hvordan ulykker kan forebygges (Engen et al., 2021, s. 159). Videre vil jeg presentere tre relevante og kjente beredskapsteorier som en del av oppgavens teoretiske rammeverk.

2.4.1 Menneskeskapte ulykker

Barry A. Turner (1978) forklarer hvordan og hvorfor ulykker skjer i organisasjoner og teknologiske systemer. Hans teori om menneskeskapte ulykker, baserer seg på at ulykker er et resultat av tekniske, sosiale, institusjonelle og administrative forhold i kombinasjon. Teorien viser at ulykker skjer på bakgrunn av vanlige og hverdagslige prosesser i organisasjoner (Turner, 1978).

Turner forklarer at i rutiner og prosedyrer i organisasjoner er det kulturelle antakelser og normer som styrer den kollektive oppmerksomheten og atferden i møte med farer og trusler. Basert på disse kulturene kan det utvikles avvik mellom antakelser om risiko og det som faktisk foregår. Turner kaller dette «informasjonsgap», noe han forklarer med flere årsaker; perseptuell rigiditet, flertydig informasjon, systematisk forbigåelse av regler og organisatorisk arroganse og selvsikkerhet. Turners teori viser at ulykker ofte inntreffer i organisasjoner som blir ansett for å ha god sikkerhet, er velfungerende og blir oppfattet som rasjonelle av samfunnet. Det er dermed vanskelig å finne åpenbare «syndebukker» i ulykker. Dersom man ser ulykkene i rammer av menneskeskapte og kollektive prosesser, kan det derimot gi mening. I etterkant av samfunnsulykker avdekkes det gjerne mangelfullt kunnskapsgrunnlag og begrensninger i organisasjonens kollektive evne til å forstå risiko, forebygge og håndtere uønskede hendelser (Turner, 1978).

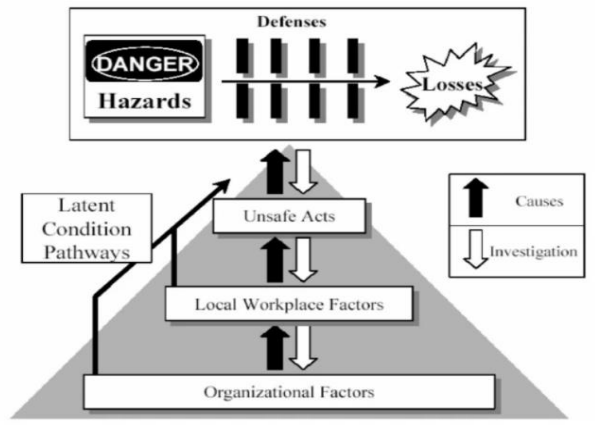
Tiden frem mot en ulykke kalles i Turners teori for «inkubasjonstid». Her vil det skje små hendelser og en rekke skjulte feil som ikke blir forstått på riktig måte fordi det ikke stemmer med organisasjonens kollektive oppfatning av hvordan ulykker skjer. Turner er opptatt av risikoforståelse, hvor han mente at alle oppfatter risiko ulikt. Turner legger med det stor vekt på betydningen av kulturen i en organisasjon og de ansattes antakelser og oppfatninger når det kommer til risiko. Dette gjør at risikovurderinger kan bli problematiske, fordi risiko blir oppfattet ulikt. Sikkerhetskulturen og risikoforståelsen til de ansatte i organisasjonen blir derfor viktig fordi feil oppfatning kan føre til ulykker (Turner, 1978).

Turners teori har lagt mye av grunnlaget for å forstå det ledelses- og kulturmessige som foregår i organisasjoner og hvordan dette kan linkes til ulykker. Turner mener at organisasjonens sikkerhetskultur gjerne reflekterer ledelsens forpliktelse og opptatthet av sikkerhet. Han er også opptatt av å utviklingen strukturer og prosesser for hvordan informasjon kan håndteres på best mulig måte. Turner mener at noen av utfordringene i organisasjoner som kan føre til ulykker er problemer med informasjon og kommunikasjon. Et eksempel på dette er at organisasjoner har manglende eller feil informasjonsformidling, for mye og for store mengder informasjon å forholde seg til, ignorering av eksisterende informasjon og at informasjonen lander hos feil personer. I arbeidet med samfunnssikkerhet må man forstå implikasjonene av menneskers begrensede rasjonalitet; vår evne til å forutse framtidige farer, for eksempel knyttet til teknologisk utvikling, vil være kontekstuell og bundet av perspektivene til øyene som ser (Turner, 1978).

2.4.2 Organisatoriske ulykker

James Reason (1997) sin teori om organisatoriske ulykker baserer seg på at det eksisterer underliggende årsaker til hvorfor en ulykke inntreffer. Han mener at det å si at alle ulykker er forskjellige og har forskjellige årsaker blir en forenklet generalisering, og at det ofte eksisterer underliggende strukturelle likheter som kan forklare ulykkene. Organisatoriske ulykker har gjerne flere årsaker og involverer mange mennesker som opererer på forskjellige nivåer i en virksomhet. Organisatoriske ulykker kan ha stor effekt også på eksterne ikke-involverte parter. Slike hendelser kan være vanskelige å forstå, kontrollere og å forutse. For å hindre at de oppstår må vi forstå hvordan de utvikler seg (Reason, 1997).

Reason har et systemisk perspektiv på årsaken til organisatoriske ulykker. Selv om vi ikke kan nekte for at menneskelige vurderinger, beslutninger og handlinger er involvert i organisatoriske ulykker, mener Reason at menneskelige feil i all hovedsak ikke skyldes individet selv, men er et resultat av forhold ved organisasjonen. I dette perspektivet ses menneskelige feilhandlinger på som en konsekvens heller enn årsak. Sentralt i Reasons teori er noe han kaller latente forhold, som er forhold som eksisterer i organisasjonen som kan skape ulykker. Dette kan dreie seg om organisering, beslutninger, ledelse, uoppdagede feil, prosedyrer og rutiner, øvelse og trening og utstyr. Slike latente forhold kan eksistere i lang tid før de kan, kombinert med den lokale situasjonen og menneskelige feil, penetrere mange lag med forsvarsbarrierer. Hver faktor for seg har ikke nødvendigvis en utløsende effekt, men kombinert kan de utløse en katastrofe (Reason, 1997, s. 10). Figur 2.1 viser stegene i utviklingen og etterforskningen av en organisatorisk ulykke.



Figur 2.1 *Stages in the development and investigation of an organizational accident.* Fra *Managing the Risks of Organizational- Accidents* (s. 17), av J. Reason, 1997, Ashgate.

Latente forhold er uunngåelige og eksisterer i alle organisasjoner. For å kunne forebygge uønskede hendelser mener Reason at man må se på de organisatoriske forholdene heller enn å se på menneskelige feil, da menneskelige feil gjerne er et resultat av de organisatoriske forholdene. De organisatoriske forholdene baserer seg gjerne på beslutninger fattet av ledere. Dette trenger ikke å være dårlige beslutninger, sett i lyset av den konteksten de er fattet i, men de kan over tid skape latente forhold i organisasjonen. Et eksempel på dette kan være at det allokeres mer penger i budsjettet til enkelte områder av de organisatoriske aktivitetene enn andre, noe som kan skape utilsiktede svakheter (Reasjon, 1997, s. 11).

Forbedringer i sikkerheten er ofte noe som skjer etter at en uønsket hendelse hat inntruffet. Et riktig fokus på sikkerhet kan gjøre at man få på plass sikkerhetsløsninger slik at ulykker kan unngås. Sikkerhetslag eller barrierer er skapt for å motstå farer. Når en uønsket hendelse inntreffer, har den kommet seg gjennom eller omgått barrierene. Konseptet forsvar-i-dybden representerer forskjellige myke og harde barrierer som er tiltak rettet mot de organisatoriske forholdene. Tanken bak dette er at det er en rekke suksessive lag av sikkerhet, hvor det ene laget dekker opp sårbarhetene i laget foran. Det er mangfoldet av overlappende og gjensidig støttende sikkerhetslagsom gjør at organisasjoner kan sikre seg mot enkle feil, enten menneskelige eller teknologiske. Harde barrierer dreier seg om tekniske tiltak og fysiske installasjoner, mens de myke barrierene dreier seg om rutiner, prosedyrer, trening og opplæring, altså forskjellige tiltak rettet mot menneskene. Forsvar-i-dybden baserer seg på en miks av både myke og harde barrierer (Reason, 1997, s. 8).

2.4.3 Høypålitelige organisasjoner

Teorien om høypålitelige organisasjoner, High Reliability Organizations (HRO), blir ofte sett på som en motpol til flere andre teorier om ulykker da den retter fokuset mot hvorvidt uønskede hendelser i organisasjoner kan forebygges, heller enn hva som forårsaker en ulykke. HRO-teorien ble utviklet av forskere ved University of California, Berkely, på 1980-tallet, og har senere blitt beskrevet av flere kjente forskere. Teorien presenterer et optimistisk syn på styring og sikkerhet ved at den har som utgangspunkt at uønskede hendelser kan forebygges og at noen organisasjoner har en unik evne til å unngå uønskede hendelser gjennom organisasjonsdesign, noe som kan kompensere for menneskelige feil og svakheter (Aven et al., 2019, s. 59).

Kjernen i teorien om høypålitelige organisasjoner er noe som kalles mindfull organizing. Sikkerhetskultur og høy pålitelighet i organisasjonen er basert på denne prosessen,

som handler om at HRO-ene er svært sensitive og med det vil tilpasse seg indikasjoner på farer og dermed unngår at små uhell utvikler seg og påvirker andre deler av et større system, noe som igjen kan føre til store problemer (Weick & Sutcliffe, 2015, s. 21-22). I det ligger det at organisasjonen oppfatter og tolker samtidig som man fatter beslutninger og handler og med dette klarer å se konturene av hva som skjer videre. Dette kalles også sensemaking (Weick & Sutcliffe, 2015, s. 32). Mindfull organizing og sensemaking henger sammen gjennom at organisering kan ses på som en prosess basert på meningsdanning gjennom persepsjon, erfaring og forventninger. Prosessen omtales som konstant meningsskapende, og legger grunnlaget for en helhetlig tilnærming til sikkerhet og motstandsdyktighet i organisasjonen (Weick & Sutcliffe, 2015, s. 35). High reliability organizations, eller organizing, er med dette en dynamisk og kontinuerlig prosess som setter HRO-ene i stand til å opprettholde sikker virksomhet over tid gjennom både å kunne forutse og eventuelt mestre uønskede hendelser, forutsette og uforutsette (Weisk & Sutcliffe, 2015). I HRO-teorien finnes det fem kognitive prinsipper for å oppnå høy pålitelighet over tid som er et produkt av mindfull organizing, sensemaking og ledelse (Weick & Sutcliffe, 2015, s. 7-14):

(1) Opptatthet av feil – handler om å identifisere og håndtere små feil og hendelser som dukker opp. Dette baserer seg på at ansatte i virksomheten er oppmerksomme på symptomer og indikasjoner på feil som kan spre seg og at disse blir tatt tak i. Hensikten er å forhindre at mange små feil som en helhet skal kunne utløse en stor uønsket hendelse.

(2) Motvillighet til å overforenkle årsaker – dette prinsippet fokuserer på at det i en virksomhet må eksistere en motvillighet til å akseptere forenklinger. Forenklinger av årsaker kan forhindre virksomheten i å se detaljene i hva som kan forårsake feil og uforventede hendelser. Dette kan også ses på som å unngå å ta snarveier og lettvinte løsninger i det daglige. Forenklinger og generelle forklaringer på komplekse kontekster og hendelser kan vanskeliggjøre det å forestille seg uønskede konsekvenser.

(3) Sensitivitet til operasjoner – det store bildet i HRO baserer seg like mye på det operasjonelle som det strategiske. Sensitiviteten til operasjoner handler om å oppdage avvik mens de fremdeles er sporbare og kan håndteres. Dette punktet er viktig for de ansatte der arbeidet gjøres og krever oppmerksomhet, bevissthet til risiko, og årvåkenhet. Dette handler om sensitivitet til det som faktisk skjer, men krever at man klarer å skille mellom forventet risiko knyttet til operasjonene og kontekst.

(4) Forpliktelse til resiliens – Ingen systemer er perfekte, og ingen er immune mot feil. For å opprettholde resiliens er det viktig at virksomheten fokuserer på å lære av sine feil,

utfordrer sine oppfatninger og fortsetter å være sensitive til operasjoner med en forpliktelse til resiliens. Essensen av resiliens er evnen til en virksomhet til å opprettholde eller gjenoppta en dynamisk og stabil situasjon som tillater organisasjonen å fortsette sin virksomhet etter en uønsket hendelse eller under stort press og stress.

(5) Anerkjennelse av kompetanse – HRO-er ønsker mangfold i sin ekspertise fordi det både bidrar til å kunne håndtere usikkerhet i forskjellige miljøer, men også fordi det hjelper dem å tilpasse seg komplekse settinger. Dette handler også om å utnytte organisasjonens ekspertise på best mulig måte. Dersom en uønsket hendelse oppstår vil det ikke alltid være ledelsen på topp som vil kunne ta de beste beslutningene, basert på kompetanse og erfaring. Gjennom å desentralisere beslutningsmyndighet slik at beslutninger kan tas i frontlinjen, og at beslutninger også skal kunne tas av dem med best ekspertise, ivaretas dette prinsippet.

2.5 Oppsummering – Kjerneelementer fra det teoretiske rammeverket

Det teoretiske rammeverket i dette forskningsprosjektet baserer seg i all hovedsak på tre sentrale og kjente teorier innen samfunnssikkerhet og beredskap. Dette er teoriene om menneskeskapte ulykker, organisatoriske ulykker og høypålitelige organisasjoner. Der te to første teoriene retter seg mot å se på hva som er årsakene til at ulykker skjer, fokuserer teorien om høypålitelige organisasjoner på hvordan man kan forebygge ulykker gjennom organisering og konstante meningsdannende kognitive prosesser. I tillegg til de sentrale beredskapsteoriene er litteraturen som treffer risikosamfunnet, risiko og risikoforståelse, sikkerhetskultur, menneskelige, teknologiske og organisatoriske forhold i arbeidet med sikkerhet, forebygging, beredskap og samarbeid i forbindelse med kriser og uønskede ondsinnede handlinger. Tabell 2.1 viser oversikt over kjerneelementene fra teorien som knytter seg til menneskelige og organisatoriske forhold. Kjerneelementene vil bli sentrale når det kommer til de empiriske funnene og oppgavens hovedfunn som drøftes i kapittel 5.

Kjerneelement	**Risiko, risikosamfunnet og risikoforståelse**	**Forebygging, beredskap, kriser og samarbeid**	**Sikkerhetskultur – MTO**	**Menneskeskapte ulykker**	**Organisatoriske ulykker**	**Høypålitelige organisasjoner**
Risikoforståelse	Risiko konstrueres av mennesket. Hvordan oppfatter vi og forstår risiko	Risikosamfunnet presenterer nye former for kriser og sårbarheter, spesielt i tilknytning til digitaliseringen og samfunnets tette kobling	Kollektiv forståelse av hva som er farlig og hvordan man kan redusere farene sentralt. Verdier kobles til nett	Organisasjoners kollektive evne til å forstå risiko. Alle oppfatter risiko ulikt. Avhengig av kultur i organisasjonen	Forståelse av hva som kan bryte gjennom forsvar i dybden og hvilke sikkerhetslag som må til	Meningsdanning gjennom persepsjon, erfaringer og forventninger. Kontinuerlig prosess

Sikkerhetskultur			Hvordan menneskene i en virksomhet forholder seg til digitale verdier og deres sikkerhetsatferd	Organisasjoners sikkerhetskultur reflekterer ledelsens forpliktelse og opptatthet av sikkerhet	Menneskelige feil som et resultat av organisatoriske forhold	Kollektivt fokus på sikkerhet i alle ledd. Oppdage feil før de utvikler seg til noe alvorlig.
Samvirke	Nye sårbarheter skapt av avhengigheter i dagens samfunn krever samarbeid	Et samfunn med nye sårbarheter og komplekse trusler må møtes med samlede tilgjengelige ressurser. Samstyring og offentlig-privat samarbeid	Mennesker, organisasjon og teknologi – samspill			
Ledelse		Samfunnssikkerhets- og beredskapsprinsipper	Ledelse essensielt for god risikostyring og sikkerhetskultur	Ledelsen sentral for hvordan en organisasjon jobber med sikkerhet	Prioritering av sikkerhet og allokering av ressurser før ulykke inntreffer. Unngå latente forhold	Forpliktelse til resiliens og anerkjennelse av kompetanse. Desentralisering av beslutningsmyndighet i gitte situasjoner
Kunnskap og kompetanse	Kunnskap om trusler, sårbarheter og verdier påvirker vår risikoforståelse	Politiets forebygging avhenger av kunnskapsgrunnlag. Forutse uønskede hendelser Kontinuerlig prosess	Kunnskap om datasikkerhet essensielt for å opprettholde sikkerhet	Manglende kunnskap og kompetanse kan føre til ulykker. Informasjonsgap. Store mengder informasjon og kommunikasjon	Kunnskap kan bidra til å prioritere sikkerhet før ulykke skjer	Anerkjennelse av kompetanse, utnyttelse av intern og ekstern kompetanse.
Helhetlig tilnærming til sikkerhet	Kunnskap om trusler, sårbarheter og verdier	Et komplekst trusselbilde krever helhetlig tilnærming og innsats	I en virksomhet må man jobbe med sikkerhetstiltak opp mot mennesker, organisasjon og teknologi	Ulykker baserer seg på tekniske, sosiale, institusjonelle og administrative forhold i kombinasjon. Krever helhetlig tilnærming	Forsvar i dybden, myke og harde barrierer	Fem kognitive prinsipper
Forebygging		Sentralt i arbeidet med samfunnssikkerhet. Gjelder både i det offentlige og private. Samspill	Tekniske sikkerhetstiltak vil ikke alene beskytte mot trusler, avhengig av sikkerhetskultur	Utvikle strukturer og prosesser for å behandle informasjon. Inkubasjonstid og avdekke feil	Unngå latente forhold i organisasjonen som kan skape ulykker	Mindful organizing og sensemaking, unngåelse av uønskede hendelser gjennom erfaring og persepsjon

Tabell 2.1 Oversikt over kjerneelementer fra det teoretiske rammeverket.

3 Metodiske momenter

Som mennesker danner vi oss enkelt generelle oppfatninger og teorier, basert på våre erfaringer og opplevelser. De generelle forestillingene er ikke alltid riktige, men gir oss forutsigbarhet og er nødvendige for at vi skal fungere i hverdagen. Vitenskapelig metode er ikke ulikt hvordan vi i det daglige tilegner oss kunnskap. Forskjellen er at vi gjennom den vitenskapelige metoden følger en fremgangsmåte. Samfunnsvitenskapelig metode handler om hvordan vi skaffer oss informasjon om den sosiale virkeligheten, samfunnsmessige forhold og prosesser. Metoden hjelper oss med å undersøke om våre antakelser og teorier er i overenstemmelse med virkeligheten eller ikke. De viktigste kjennetegnene ved metoden er systematikk, grundighet og åpenhet (Johannessen, Tufte & Christoffersen, 2020, s. 19-22).

Forskningsprosessen går vanligvis over fire faser; forberedelse, datainnsamling, dataanalyse og rapportering. En studie starter som regel med at man ønsker kunnskap om en virkelighet, som gjerne formuleres som en problemstilling. Forberedelsesfasen omfatter å ta stilling til forskningens formål, og her blir arbeid med problemstillingen sentralt da den viser hva undersøkelsen skal gi svar på. Problemstillingen legger videre føringer for valg av teori, forskningsdesign og metode (Johannessen et al., 2020, s. 23 og s. 33). Min problemstilling er som følger: *Hvilke faktorer påvirker norske virksomheters samarbeid med politiet når det kommer til forebygging og håndtering av datakriminalitet?*

For å undersøke problemstillingen min nærmere utformet jeg også forskningsspørsmål. Gjennom disse spørsmålene vil jeg se nærmere på hvordan politiets arbeid med datakriminalitet og virksomhetenes beredskapsarbeid påvirker samarbeidet mellom virksomhetene og politiet, hva som ligger til grunn for virksomhetenes beslutning om å kontakte politiet i forbindelse med datakriminalitet, hvilke forventninger virksomhetene har til politiet når det kommer til forebygging og håndtering av datakriminalitet, hva politiet kan gjøre for å legge bedre til rette for et samarbeid med virksomhetene og hvilken rolle samfunnet og media spiller i samarbeidet mellom virksomhetene og politiet. Det er mange fremgangsmåter man kan benytte i et forskningsprosjekt. I dette kapitlet vil jeg redegjøre for hvordan jeg har gått frem for å finne relevant litteratur og teori, hvilke vurderinger og valg jeg har gjort når det kommer til forskningsdesign og metode, teknikken jeg har brukt for datainnsamling, valg av informanter og fremgangsmåte for analyse av forskningsdata. Jeg vil også reflektere rundt validitet, pålitelighet, generalisering og egen rolle som forsker.

3.1 Forskningsdesign og metode

I forskningens forberedelsesfase må det tas stilling til hvem og hva som skal undersøkes, og hvordan undersøkelsen skal gjennomføres. Dette kalles forskningsdesign, og det dreier seg om hvordan man skal gå frem for å besvare problemstillingen (Johannessen et al., 2020, s. 55-56; Blaikie, 2010, s. 15). Ut fra min problemstilling ønsket jeg å få dypere innsikt i hvilke faktorer som påvirker samarbeidet mellom store norske virksomheter og politiet når det kommer til forebygging og håndtering av datakriminalitet. Jeg ønsket med det å undersøke et spesifikt fenomen og få mer detaljert og nyansert informasjon om dette slik det oppleves av personer som jobber med sikkerhet i virksomhetene og personer som jobber med tematikken representert av politiansatte og personer ansatt i offentlige myndighetsorganer og private sikkerhetsselskaper. Med bakgrunn i dette valgte jeg å gjennomføre en deskriptiv og til dels komparativ casestudie med flere caser, gjennom at jeg undersøkte hvordan fenomenet oppleves av relevante personer i forskjellige norske virksomheter og blant mennesker som jobber med sikkerhet i det offentlige og det private, for å sammenligne og se fenomenet fra flere sider. Dette kalles også en flercasestudie (Johannessen et al., 2020, s. 211-213). Studien ble også til en viss grad eksplorativ gjennom at fenomenet ikke er forsket mye på tidligere, og jeg ville komme til å finne mønstre og strukturer som ikke er omfattet i eksisterende teorier (Blaikie, 2010, s. 71). Studien ble gjennomført som en tverrsnittsundersøkelse da formålet var å undersøke hvordan situasjonen er her og nå. Samtidig begrenser en masteroppgave seg i tid og omfang (Johannessen et al., 2020, s. 55). Informasjonen fra datainnsamlingen viste tilstanden på et gitt tidspunkt. Datainnsamlingen i min studie pågikk i en periode på ca. en og en halv måned i starten av 2022.

I den samfunnsvitenskapelige metodelæren går det et skille mellom kvantitative og kvalitative metoder. I en kvantitativ tilnærming kan man for eksempel telle opp fenomener for å kartlegge utbredelse, mens i en kvalitativ tilnærming vil vi få mer detaljert og utfyllende informasjon om et fenomen. Innen kvalitative forskningsmetoder ligger fokuset gjerne på å forstå heller enn å forklare (Johannessen et al., 2020, s. 22-23, Tjora, 2012, s. 18). Metodene kan benyttes i kombinasjon. Hvorvidt dette er hensiktsmessig og gjennomførbart avhenger av problemstilling, undersøkelsens formål, valg av forskningsdesign og tid og ressurser til rådighet. Dersom man benytter begge metodene er gjerne målet å sammenligne to sett med resultater, eller oppveie svakheter i både kvantitative og kvalitative metoder ved å utnytte styrkene til begge metodene (Johannessen et al., 2020, s. 256). Casestudier kan med fordel gjennomføres ved å kombinere metodene da dette vil kunne gi mye og detaljert data

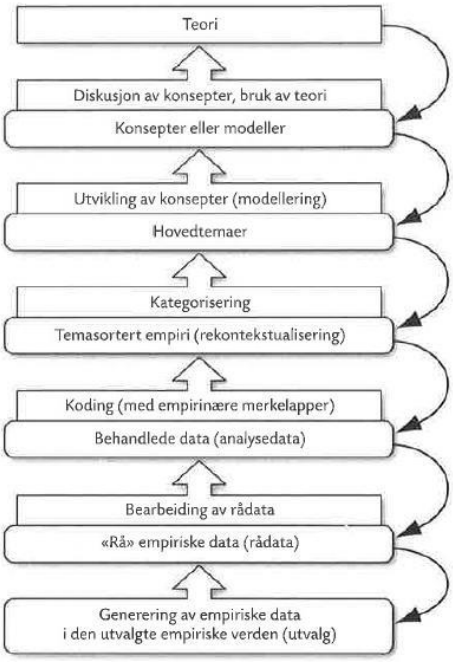
(Johannessen et al., 2020, s. 212). Selv om en kombinasjon av metodene utvilsomt kunne gitt et bredt datagrunnlag hvor jeg i tillegg kunne ha veid opp svakhetene i den ene metoden med styrker fra den andre, valgte jeg å gå får en kvalitativ tilnærming. Siden formålet med undersøkelsen var å få detaljert og utfyllende informasjon for å forstå fenomenet vurderte jeg at det var mest hensiktsmessig å besvare problemstillingen gjennom en kvalitativ metode, hvor jeg heller valgte ut færre informanter samtidig som jeg gikk dypere inn i forståelsen for fenomenet. I tillegg ville en kombinasjon av metodene vært svært tidkrevende, og en masteroppgave setter begrensninger når det kommer til både tid og ressurser.

Formålet med den kvalitative analysen er å gjøre det mulig for en leser av forskningen å få økt kunnskap om saksområdet det forskes på, uten selv å måtte gå gjennom datamaterialet fra datainnsamlingen (Tjora, 2012, s. 174-176). Det finnes flere metoder å jobbe etter når det kommer til forskningsprosess og teknikker for både å samle inn data og arbeide med disse. Flere metoder har også overlappende elementer eller baserer seg på liknende konsepter og tilnærminger. Relasjonen mellom teori og empiri i en undersøkelse kan dreie seg om å ta utgangspunkt i en teori og ved hjelp av data enten få bekreftet eller avkreftet teorien. Å gå fra teori til empiri kalles deduksjon. En annen strategi er å starte undersøkelsen uten et teoretisk utgangspunkt og samle inn data med et formål om å finne frem til generelle mønstre som kan utlede teorier eller generelle begreper. Dette kalles induksjon, altså fra empiri til teori. Når man veksler mellom tilnærmingene kalles det abduksjon (Johannessen et al., 2020, s. 28-30).

Metoden Grounded Thoery (GT) egner seg når man ønsker å undersøke et felt man ikke kjenner så godt fra før og formålet er å kartlegge, beskrive og forstå fenomenet. Hovedideen bak denne forskningsmetoden er å utvikle nye teoretiske ideer som har basis i datamaterialet, altså en induktiv tilnærming (Nilssen, 2012, s. 78-79). GT har et ideal om et teorifritt utgangspunkt for den kvalitative forskningen, med en strategi der teoriutvikling baserer seg på systematisk sirkulær vandring mellom datagenerering og utvikling av konsepter (Tjora, 2012, 25-30). En annen metode som ikke er ulik GT, er den stegvis-deduktive induktive metoden (SDI) som tar sikte på å utvikle konsepter, modeller eller teorier gjennom å arbeide i «etapper» fra rådata til konsepter eller teorier. Den oppadgående prosessen er induktiv. De nedadgående tilkoblingene er deduktive ved at man sjekker fra det mer teoretiske til det mer empiriske. I GT kalles dette theroetical sampling, altså at man i konseptutviklingen får behov for mer empiri for å komme videre. Likevel kan det argumenteres for at det ofte i forskningsprosjekter ikke er tid til å veksle mellom datagenerering og konseptutvikling slik

meningen er i GT og at det ofte i forskningsprosjekter heller er snakk om en mer generell induktiv metode som SDI (Tjora, 2012, s. 174-176).

SDI-modellen viser kvalitativ forskning som etapper, noe som er ment for å støtte oppunder systematikken i forskningen. Likevel vil man i praksis kunne være på ulike stadier i SDI-modellen samtidig for ulike deler av et prosjekt. Hovedformålet med denne modellen er å ta ut potensialet i empirien man har fremskaffet og ikke basere seg på å fremskaffe ytterligere data ettersom man har behov for det (Tjora, 2012, s. 174-176). SDI-modellen ligger tett opptil en abduktiv strategi da både induktiv og deduktiv fremgangsmåte er sentralt i prosessen (Tjora, 2012, 25-30). Jeg har valgt case som mitt forskningsdesign med bakgrunn i at jeg ønsker å undersøke flere caser. Her blir casene både studieobjekter og fremgangsmåte. Jeg har også valgt å basere fremgangsmåten min med utgangspunkt i GT, da jeg ønsket å undersøke et felt jeg ikke kjente så godt fra før av og som det ikke eksisterte mye teori på, og formålet mitt var å kartlegge, beskrive og forstå fenomenet. Tiden jeg hadde til rådighet for studien gjorde det vanskelig å legge til rette for å kunne hente inn ytterligere empiri ved behov, noe som gjorde at jeg måtte basere meg på det empiriske grunnlaget jeg fikk gjennom datainnsamlingen. På den måten fant jeg SDI-modellen hensiktsmessig da jeg så at jeg ville jobbe i flere av «etappene» samtidig gjennom å drive datainnsamling og utforske teori og empiri om hverandre. Figur 3.1 viser de forskjellige etappene i SDI-modellen.



Figur 3.1 *Stegvis-deduktiv induktiv metode (SDI).* Fra *Kvalitative forskningsmetoder i praksis* (s.175), av A. Tjora, 2012, Gyldendal Norsk Forlag

Mens data, eller empiri, er konkrete representasjoner av den sosiale virkeligheten, er teorier uttrykk for mer generell kunnskap og antakelser om virkeligheten. Vitenskapelig teoretisering handler om generalisering, å gjøre konkrete fenomener allmenne (Johannessen et al., 2020, s. 28-30). Et spørsmål man kan stille når det kommer til GT og SDI er hva som skal til for å kalle noe en teori. De strengeste kravene er sier at teorier skal være et sett av lover, som sjeldent finnes i samfunnsvitenskapen, mens et annet syn sier at en teori kun er en måte å forstå noe på. Sistnevnte gjør at en teori og et konsept blir ganske likt hverandre. SDI-modellen operere med både konsepter og teorier. En tilnærming til dette er å si det som at en teori må være falsifiserbar eller prøvbar. I store deler av samfunnsforskningen vil man stoppe ved konsepter og anse dette som legitime resultater. Konseptualisering eller konseptuell generalisering er derfor normalt innen mindre forskningsprosjekter. I større prosjekter bør teoretisk utvikling en relevant ambisjon (Tjora, 20212, s. 189-191). I forskningsprosjektet mitt vil SDI være metoden jeg benytter i prosessen. Da jeg har et mindre forskingsprosjekt vil resultatene ikke resultere i produksjon av ny teori, men forskningsprosessen vil likevel kunne lede til konseptualisering eller konseptuell generalisering.

Innen kvalitativ forskning legges det ofte vekt på at teori ikke skal styre forskningen. Likevel kan vi argumentere for at forskere alltid har med seg en type forforståelse. Egen fagdisiplin vil alltid ha en innvirkning på hva slags fenomen man er opptatt av, og hvordan man forsker på disse (Tjora, 2012, 25-30). Når man skal gjennomføre en undersøkelse vil man ha med seg et teoretisk rammeverk, altså teorien som omgir studien, som gjerne blir utledet fra forståelsen og holdningen forskeren har med seg. Avhengig av teoretisk innfallsvinkel til studien vil vi stille ulike spørsmål, og man vil ikke nødvendigvis se det samme. Dette påvirker våre tolkninger, hvilke spørsmål som stilles og hvilke teorier og dokumenter man velger å se på. I tillegg til teorien vil vi i datainnsamlingen møte det nye og ukjente med bakgrunn i det tankesettet vi har fra før, noe som kan kalles forforståelse. Det omfatter ikke bare det teoretiske rammeverket, men også forskerens erfaringer, verdier, holdninger og kunnskap (Nilssen, 2012, s. 61-68). Da jeg bestemte meg for å ha samarbeid mellom norske virksomheter og politiet når det kommer til forebygging og håndtering av datakriminalitet som tema for oppgaven, var det med bakgrunn i egne observasjoner, erfaringer og antakelser om at dette samarbeidet i dag er utfordrende, samtidig som det er sentralt når det kommer til å møte truslene som datakriminalitet utgjør mot samfunnet vårt. Grunnlaget for at dette samarbeidet er utfordrende knyttes til virksomhetenes arbeid med sikkerhet- og beredskap, og kapasiteten og kompetansen til politiet når det kommer til datakriminalitet. Etter å ha studert

beredskap og kriseledelse er jeg godt kjent med teorier innen organisatoriske- og menneskeskapte ulykker, samt grunntankene bak arbeid med beredskap og viktigheten av samarbeid på tvers av sektorer når det kommer til å opprettholde god samfunnssikkerhet. I tillegg har jeg bakgrunn fra politiet og andre offentlige myndigheter hvor arbeidet med sikkerhet og beredskap står sentralt. Denne bakgrunnskunnskapen dannet min forforståelse til undersøkelsen, og spilte inn på utgangspunktet for arbeidet med forskningsprosjektet, utarbeidelsen av intervjuguiden og hvordan jeg fant relevant teori. Samtidig var utfordringene knyttet til samarbeid mellom de norske virksomhetene og politiet og utfordringene knyttet til datakriminalitet noe, jeg ikke kunne veldig mye om og derfor måtte utforske mer.

3.2 Datainnsamling og utvalg

Formålet med å bruke en kvalitativ metode for datainnsamling er å få mer detaljert og utfyllende informasjon om fenomenet som undersøkes. Derfor er det sentralt å vurdere hvem som skal delta i undersøkelsen, hvor mange informanter man trenger og hvilken utvalgsstrategi som bør benyttes i rekrutteringen for å komme i kontakt med personer i den målgruppen man er interessert i å vite noe om (Johannessen et al., 2020, s. 23-24). Kvalitative metoder samler inn og registrerer data i form av tekst, lyd og bilder, og det er tre grunnleggende forskjellige måter å samle inn dataene på; observasjon, intervju og dokumentanalyse (Johannessen et al., 2020, s. 54). For å få så detaljert og utfyllende informasjon som mulig om temaet jeg ønsket å undersøke og virkelig forstå fenomenet, ble det tidlig klart for meg at jeg ønsket å samle inn data gjennom intervjuer. For å se hva slags informasjon jeg trengte og hvor jeg kunne få tak i informasjonen ble det sentralt å spisse problemstillingen slik at den ble aktuell og forskbar. For å utfordre mine egne antakelser og oppfatninger rundt temaet gjennomførte jeg samtaler med kollegaer og venner, og leste også om tematikken i forskjellige medieoppslag, trussel- og risikovurderinger, undersøkelser og andre offentlige dokumenter. Jeg begynte med en ganske bred tilnærming til temaet, og etter hvert som jeg snakket med folk og leste meg opp klarte jeg å snevre inn og konkretisere problemstillingen, slik at forskningsprosjektet ble realistisk å gjennomføre med tanke på tid og ressurser, og jeg fikk klarhet i hvordan jeg skulle gå frem for å samle inn data. Jeg forstod raskt at avgrensning og nøye vurderinger rundt spissing av tema og utvalg av informanter kom til å bli svært viktig for at jeg skulle få gjennomført forskningsprosjektet.

Ofte er det fenomenet vi ønsker å studere såpass omfattende at det vanskelig lar seg studere i full dybde og bredde, derfor er det nødvendig å avgrense (Johannessen et al., 2020, s.

37). Som utgangspunkt for oppgaven ønsket jeg å ha offentlige virksomheter og virksomheter i forskjellige størrelser som målgruppe, noe som raskt endret seg etter at jeg hadde gjennomført de innledende samtalene med kollegaer og venner. Å undersøke fenomenet såpass bredt hadde rett og slett blitt for tidkrevende og omfattende. Jeg begrenset det så til å kun gjelde norske virksomheter og ikke offentlige virksomheter, og forstod raskt at jeg ble nødt til å avgrense det enda mer. Etter gode råd fra veileder og kollegaer landet jeg på at målgruppen for utvalg 1 ble store norske virksomheter. Bakgrunnen for dette var en antakelse om at store norske virksomheter har kommet lenger i arbeidet med digital sikkerhet enn de små og mellomstore virksomhetene, og har allerede gått noen runder når det kommer til samarbeid med politiet og åpenhet relatert til mindre alvorlig og alvorlig datakriminalitet. Det var enklere å avgrense i utvalg 2, da jeg her ville snakke med personer i politi- og lensmannsetaten, offentlige myndighetsorganer og private sikkerhetsselskaper som jobber med digital sikkerhet og datakriminalitet og har erfaring fra et privat-offentlig samarbeid.

3.2.1 Utvalgsstrategi

Begrensninger i tid og ressurser gjør det ekstra viktig å nå frem til informanter som kan gi god informasjon. Gjennom datainnsamlingen skulle jeg ikke generalisere fra utvalget til en populasjon, men forklare, beskrive og tolke fenomenet jeg forsket på. Derfor ble det viktig å komme i kontakt med informanter som hadde god informasjonsrikdom, samtidig som jeg ikke måtte ha så mange informanter at jeg ikke klarte å gjennomføre prosjektet (Johannessen et al., 2020, s. 74). Strategisk utvelgelse vil si at man tenker nøye gjennom hvilken målgruppe som vil gi nødvendige data. Videre vil man velge ut personer fra målgruppen som skal delta i undersøkelsen (Johannessen et al., 2020, s. 57-58; Tjora, 2012, s. 145). Å studere et fenomen i forskjellige kontekster kan gi robuste funn og åpner for sammenligning og muligheten for å se fenomenet fra flere forskjellige sider (Johannessen et al., 2020, s. 213). Etter samtalene jeg hadde med kollegaer og venner om temaet jeg valgte for oppgaven kom jeg frem til at jeg ønsket å ha med to forskjellige intervjuutvalg i studien. Bakgrunnen for dette var at jeg skulle studere samarbeidet mellom to forskjellige parter, og jeg anså det dermed som hensiktsmessig med to forskjellige intervjuutvalg for å forstå fenomenet. Jeg har selv bakgrunn og erfaring fra forskjellige offentlige myndighetsorganer hvor datakriminalitet og sikkerhet står sentralt. Da jeg ikke ønsket å kun bruke mine egne erfaringer inn i studien, men heller innta en mer objekt rolle som forsker, ønsket jeg å intervjue personer som jobber med tematikken i det daglige i politi- og lensmannsetaten, andre offentlige myndighetsorganer og i private sikkerhetsselskaper. I tillegg ønsket jeg å snakke med personer i forskjellige norske

virksomheter innenfor ulike bransjer for å få et bredt bilde av temaet fra virksomhetenes side. De to intervjuutvalgene vil jeg heretter vil omtale som utvalg 1 og utvalg 2. I utvalg 1 endte jeg opp med elleve informanter som jobber i store norske virksomheter innen bransjene matproduksjon, eiendom, finans, industri, media, salg og teknologi og innovasjon, og i utvalg 2 endte jeg opp med syv informanter innen politi- og lensmannsetaten, offentlige myndighetsorganer og private sikkerhetsselskaper.

I casestudier er analyseenhetene det som er i fokus for analysen, mens datainnsamlingsenhetene er de informantene man intervjuer. Analyseenhetene henger tett sammen med problemstillingen. I undersøkelsen min ble analyseenhetene virksomhetene i utvalg 1 og de offentlige myndighetsorganene og de private sikkerhetsselskapene i utvalg 2 og datainnsamlingsenhetene er intervjuobjektene (Johannessen et al., 2020, s. 214). Det vil i et flercasestudium være vesentlig å finne frem til informanter innenfor de forskjellige casene som på best mulig måte kan legge frem grundige beskrivelser og betraktninger knyttet til tema og case (Tjora, 2012, s. 149). For at informantene skulle være relevante for undersøkelsen måtte de oppfylle bestemte kriterier. Jeg benyttet derfor kriteriebestemt utvelgelse da jeg gikk frem for å finne aktuelle informanter (Johannessen et al., 2020, s. 64). Kriteriene for utvalg 1 var at informantene måtte jobbe med sikkerhet, herunder digital sikkerhet, for en stor norsk virksomhet, og ha en sentral rolle i arbeidet med beredskap og spille en rolle i vurderingene virksomheten gjør rundt samarbeid med politiet. Kriteriene for utvalg 2 var at informantene måtte jobbe med digital sikkerhet og ha kjennskap til datakriminalitet og offentlig-privat samarbeid.

I en flercasestudie vil man gjerne få frem en variasjonsbredde. Ulike caser, her de norske virksomhetene, politi- og lensmannsetaten, offentlige myndighetsorganer og private sikkerhetsselskaper, ville kunne gi relevant informasjon for det samme fenomenet og bidra til å se fenomenet fra «begge sider» (Tjora, 2012, s. 149). Det eksplorerende elementet i min undersøkelse ønsket å søke et relativt bredt tilfang av data gjennom å intervjue personer med tilknytning til forskjellige virksomheter og bransjer, men innenfor det samme temaet og fenomenet (Tjora, 2012, s. 148). For å sikre variasjonsbredde i utvalg 1 startet jeg med å kartlegge store norske virksomheter innen forskjellige bransjer som kunne være aktuelle for deltakelse i intervju. Jeg kontaktet virksomhetene gjennom e-post og var nøye med å beskrive hva studien gikk ut på, samt hvilke informanter jeg var ute etter å få intervjuet og kriteriene de måtte oppfylle (se vedlegg 1). Hvilke personer jeg ville komme i kontakt med var på den ene siden utenfor min kontroll, men jeg gikk ut fra at en god beskrivelse av kriteriene jeg så etter

for informantene ville gjøre at analyseenhetene vill finne relevante personer til studien. Det var ikke viktig hvilken stilling eller bakgrunn personene hadde, men at de jobber med sikkerhet, herunder digital sikkerhet, og at de vil spille en sentral rolle når det kommer til samarbeid og kontakt mellom politiet og virksomhetene når det kommer til arbeidet med digitale trusler og datakriminalitet. Jeg sendte ut mange e-poster til forskjellige virksomheter. Det varierte hvor raskt jeg fikk svar, men jeg opplevde at virksomhetene var positive til å bidra til undersøkelsen da de fleste virksomhetene anså temaet som relevant og viktig.

Utfordringen med å rekruttere informantene i utvalg 1 på denne måten var at jeg var usikker på om erfaringene til informantene jeg klarte å rekruttere ville dekke informasjonsbehovene mine. Rekruttering av informanter til en studie kan være vanskelig, og man kan sitte igjen med en følelse av at det er erfaringer man ikke får undersøkt. Man vil ikke kunne ha kontroll på hva informanter som ikke deltok i undersøkelsen ville ha sagt i intervjuene. Samtidig var jeg fornøyd med den bredden jeg fikk i utvalg 1, og opplevde da jeg intervjuet at informantene kom med mye og god informasjon (Tjora, 2012, s. 147-148).

Snøballmetoden er en utvalgsstrategi som baserer seg på at man begynner med et lite utvalg «førstekontakter» som gradvis vokser ved at forskeren får tips om nye informanter fra førstekontaktene (Tjora, 2012, s. 151). Jeg benyttet denne utvalgsstrategien til rekruttering av informanter i utvalg 2, og til dels i utvalg 1. Jeg startet datainnsamlingen med intervjuer av informanter i utvalg 2, da jeg gjennom arbeidsplassen min visste om noen sentrale personer jeg gjerne ville intervjue. Disse ga gode tips om andre informanter jeg burde kontakte, og på denne måten rekrutterte jeg flere av informantene i utvalg 2. Gjennom samtaler med kollegaer og venner fikk jeg også tips om informanter til utvalg 1. Det var mest utfordrende å rekruttere informanter til dette utvalget, og jeg opplevde det som stor hjelp å kunne kontakte informantene ved å sende en direkte e-post og referere til en kontaktperson.

Det er viktig å reflektere over hvorfor informanter melder seg frivillig til å delta i dybdeintervjuer. Informantene får muligheten til å snakke ut om et tema de er opptatte av. Dersom informantene har en skjult agenda og oppgir konkret informasjon av en spesiell grunn kan dette svekke studien (Tjora, 2012, s. 153). Alle informantene jeg har vært i kontakt med har vært positive til å bidra i forskningsprosjektet og har kommet med mye god informasjon. Jeg opplevde at informantene valgte å delta i studien fordi temaet for studien min var noe de anså som viktig, og hadde et ønske om å bidra for å belyse utfordringer og bakenforliggende årsaker i samarbeidet mellom norske virksomheter og politiet når det kommer til forebygging og håndtering av datakriminalitet, slik at samarbeidet kan bli bedre i fremtiden.

Det er i teorien ingen øvre eller nedre grense på antall informanter i en kvalitativ undersøkelse, men en god regel er at man har nok informanter når man har kommet til et datametningspunkt, altså at man ikke lenger får noe ny informasjon. Et annet moment er at antall informanter heller ikke bør overstige det som er gjennomførbart med tanke på tid og ressurser. Etter datainnsamlingen skal det også gjennomføres grundige analyser som tar tid (Johannessen et al., 2020, s. 74). Det var utfordrende å vite hvor mange informanter som var nok. Grunnet tid til rådighet hadde jeg ikke anledning til å se an om jeg nådde et datametningspunkt før jeg begynte på datainnsamlingen, derfor måtte jeg forsøke å lande på et antall i begge utvalgene som var gjennomførbart. Totalt fra begge utvalgene ble det 18 informanter. På den ene siden kan jeg si at jeg opplevde et datametningspunkt i utvalg 1 med 11 informanter da jeg begynte å se at mye av den samme informasjon gikk igjen i intervjuene. Samtidig kom informasjonen med forskjellige perspektiver og jeg opplevde til stadighet å forstå fenomenet på nye måter. Sånn sett vil jeg si at det var et passende antall informanter. I utvalg 2 opplevde jeg at jeg kunne hatt flere informanter fra flere offentlige myndighetsorganer for å få et enda bredere perspektiv og en bedre forståelse. Dersom jeg skulle gjennomført datainnsamlingen på nytt ville jeg ha vurdert å også få med informanter fra Politihøgskolen som kunne ha sagt noe om hvilken kunnskap om datakriminalitet de nyutdannede møter arbeidslivet med. I tillegg kunne det vært interessant å intervjue polititjenestepersoner fra flere politidistrikter som kunne fortalt mer om hvordan fenomenet oppleves i flere deler av politi-Norge, da informantene i min undersøkelse arbeider i store og sentrale politidistrikter. Samtidig opplevde jeg å få nok og tilfredsstillende informasjon fra utvalg 2 til å forstå fenomenet fra dette perspektivet. I tillegg til at det var utfordrende å beregne antall informanter visste jeg at jeg skulle skrive oppgaven alene innenfor en bestemt tidsramme. Tids- og kapasitetsaspektet ble derfor også viktige kriterier.

3.2.2 Intervju

Kvalitative intervjuer egner seg når man ønsker fyldige og detaljerte beskrivelser av informantenes forståelse, følelser erfaringer, oppfatninger, meninger, holdninger og refleksjoner knyttet til et fenomen, og er en vanlig datagenereringsmetode innen kvalitativ forskning (Johannessen et al., 2020, s. 106). Sosiale fenomener er komplekse, og det kvalitative intervjuet egner seg godt for å få frem kompleksiteter og nyanser (Johannessen et al., 2020, s. 108). Jeg anså intervju som en god datainnsamlingsmetode basert på problemstillingen og formålet med undersøkelsen. Jeg ønsket å snakke med mennesker som

kunne fortelle meg om deres erfaringer, opplevelser og refleksjoner slik at jeg bedre kunne forstå fenomenet.

De kvalitative intervjuene kan være mer eller mindre strukturerte hvor det ustrukturert intervjuet skaper en uformell og trygg arena for intervjuobjektet gjennom en åpen og fleksibel samtale. Det strukturerte intervjuet er gjerne mer styrt av en detaljert intervjuguide og kan oppleves mer formelt. Det gir heller ikke like mye rom til en åpen og fri dialog (Johannessen et al., 2020, s. 108). Jeg valgte å gjennomføre semistrukturerte dybdeintervjuer da dette ville gi muligheten for en relativt fri samtale hvor vi kunne kretser rundt noen spesifikke forhåndsbestemte temaer knyttet til problemstillingen og forskingsspørsmålene. Intervjuguiden satte rammene og utgangspunktet for intervjuet, samtidig som jeg kunne tilpasse rekkefølgen på spørsmålene og temaene avhengig av hvordan samtalen utfoldet seg. Jeg anså det likevel som viktig å starte intervjuene med et åpent spørsmål som gikk ganske dirkete på kjernen av temaet for undersøkelsen min. Dette gjorde jeg for at ikke informantenes svar skulle farges av den samtalen vi hadde og at informantene på et tidlig tidspunkt i intervjuet fikk mulighet til å gå i dybden der de hadde mye å fortelle. I intervjusituasjonen er det også vanlig å tillate digresjoner fra informantene noe som gir muligheten for å komme inn på temaer eller momenter som intervjueren kanskje ikke hadde tenkt på, men som kan introdusere viktige og interessante vinklinger på fenomenet som undersøkes. I intervjuet har man anledning til å stille åpne spørsmål slik at informanten kan formulere seg med egne ord om emnet og ikke med ord som forskeren allerede har gitt som alternativer (Tjora, 2012, s. 104-105; Johannessen et al., 2020, s. 108).

Dersom man skal sammenligne svarene fra intervjuene kan strukturerte intervjuer lette dette arbeidet. Jobben med å sammenligne dataene fra intervjuene ble likevel ikke en direkte sammenligning, men jeg så etter mønstre, sammenfallende og inkonsistent informasjon i datamaterialet som kunne besvare problemstillingen min. Sammenligningen ble sånn sett en del av analysen (Johannessen et al., 2020, s. 108). Intervjuene jeg gjennomførte ble basert på en semistrukturert tilnærming, men likevel med en viss grad av struktur for å sikre at vi kom inn på alle temaene som var viktig å belyse. Denne fremgangsmåten gjorde det også mulig å ha god oversikt under intervjuene slik at jeg enklere kunne la intervjuobjektene fortelle fritt, samtidig som jeg på en god måte kunne veksle mellom temaene og la intervjuet utvikle seg slik som det ble naturlig i hvert enkelt intervju. Intervjuguiden jeg utarbeidet var semistrukturert, men også med mer strukturerte spørsmål som jeg kunne trekke inn der det trengtes. Intervjuguiden fikk da overordnede temaer med åpne spørsmål, men også flere

strukturerte spørsmål under temaene (se vedlegg 4 og 5). Temaene og spørsmålene jeg valgte å ta med tok utgangspunkt i min kunnskap om tematikken og problemstillingen. Etter noen intervjuer ble det tydelig at ikke alle temaene og spørsmålene var like relevante for å besvare problemstillingen. Jeg valgte derfor å endre litt på intervjuguiden underveis ved å spisse den, noe som ga meg muligheten til å gå enda dypere inn i de teamene som virkelig ga god informasjon til oppgaven.

Før jeg startet å intervjue gjennomførte jeg et par «tester» av intervjuguiden på en venn og en kollega som begge har god kjennskap til tematikken. Hensikten med dette var å få innspill til eventuelle endringer eller tilleggsspørsmål jeg burde ta med, og at jeg som intervjuer skulle bli trygg på intervjuguiden min (Johannessen et al., 2020, s. 114). Når man jobber med et prosjekt over tid er det enkelt å ikke klare å stille seg kritisk til eget arbeid og jeg ønsket å få blikk utenifra for å sikre at jeg traff godt med intervjuguiden da det var svært viktig å få frem god informasjon i hvert intervju. Ingen av de jeg testet intervjuguiden på hadde innspill som førte til store endringer, men jeg fikk noen gode tips om rekkefølge på spørsmålene som gjorde intervjuguiden bedre. Videre fikk jeg også tips om at det var lurt å gjennomføre noen intervjuer for så å gjøre en vurdering av om intervjuguiden fungerte slik at jeg kunne gjøre justeringer tidlig i intervjuprosessen. Som beskrevet i avsnittet over gjorde jeg noen små endringer, men kun på hvilke spørsmål jeg hadde med, ikke på innhold.

Når man intervjuer til et forskningsprosjekt avhenger informasjonen som kommer ut av intervjuet av relasjonen mellom intervjueren og intervjuobjektet. Relasjonen kan påvirkes av en rekke forhold (Johannessen et al., 2020, s. 114). For å legitimere undersøkelsen var jeg nøye med å gi intervjuobjektene god informasjon om prosjektet gjennom å sende ut et informasjonsskjema. Jeg startet også intervjuene med å gi informantene muligheten til å stille spørsmål til informasjonen de hadde fått og til å forsikre meg om at de var kjent med sine rettigheter og hva de skulle være med på. Videre ble det viktig å informere om hvor lang tid intervjuet ville ta og hvordan det kom til å bli gjennomført. Situasjonen rundt intervjuet dreier seg om hvor og hvordan intervjuet gjennomføres. I utgangspunktet hadde jeg tenkt til å la intervjuobjektet bestemme sted. Da de fleste ønsket å gjennomføre intervjuet i ukedager og i arbeidstid hadde det blitt naturlig at jeg hadde kommet til intervjuobjektets arbeidsplass eller til et sted i nærheten hvor vi kunne prate uforstyrret. Jeg fikk gjennomført et par intervjuer på denne måten, men siden de fleste intervjuene ble gjennomført i en periode hvor det var anbefalt hjemmekontor grunnet Covid-19 pandemien ble majoriteten av intervjuene gjennomført digitalt via en plattform intervjuobjektet var kjent med og trygg på. Før jeg kom i

gang med intervjuene var jeg redd for at dette kunne spille inn på om intervjuobjektene ville føle seg trygge i intervjusituasjonen og på den måten påvirke informasjonen jeg fikk. Denne antakelsen ble imidlertid raskt motbevist, og jeg opplevde ikke at dette påvirket intervjusituasjonen på en negativ måte. At jeg kunne gjennomføre intervjuene på den måten førte heller til stor grad av fleksibilitet. I tillegg var jeg nok heldig med at intervjuobjektene hadde blitt godt vant til situasjonen med hjemmekontor og med det blitt trygge på å ha digitale møter. Videosamtalene gjorde også at jeg kunne observere mimikk og reaksjoner, og at både intervjuobjektene og jeg fikk opplevelsen av å snakke «ansikt til ansikt». Jeg tok intervjuene på lyd noe som gjorde at jeg i større grad kunne konsentrere meg om intervjuet. Jeg forklarte hvordan jeg skulle bruke lydklippet i etterkant av intervjuet og hvordan lydklippet ville bli oppbevart slik at de kunne føle seg trygge på at det at det ble tatt på lyd ikke ville gjøre noen forskjell på hvor åpne de kunne være. Ingen av informantene hadde noen innsigelser til dette (Johannessen et al., 2020, s. 114-116; Tjora, 2012, s. 110-112).

Semistrukturerte intervjuer settes gjerne opp med sikte på å gå gjennom tre faser; oppvarming, refleksjon og avrunding. I de forskjellige fasene stilles ulike typer spørsmål. Jeg startet intervjuene med noen oppvarmingsspørsmål som rettet seg mot intervjuobjektene, noe som ga meg god informasjon om hvert intervjuobjekt, deres perspektiver og standpunkt i tematikken. Tanken bak dette var både å la ikke starte «rett på», men heller starte med enkle og «ufarlige» spørsmål som ville gi meg innblikk i intervjuobjektets utgangspunkt for intervjuet da alle intervjuobjektene hadde forskjellig arbeidsplass, bakgrunn og rolle. Disse spørsmålene ville også kunne bidra til trygghet hos informanten. Videre fortsatte jeg med refleksjonsspørsmål hvor informanten fikk muligheten til å gå i dybden av de forskjellige temaene jeg ønsket å få informasjon om. Her opplevde jeg stor forskjell hos de forskjellige intervjuobjektene. Noen ble stilt det første refleksjonsspørsmålet som var et åpent spørsmål om samarbeid mellom norske virksomheter og politiet når det kommer til datakriminalitet. Noen snakket seg så nesten gjennom resten av intervjuguiden, mens andre stoppet opp og ble stilt oppfølgingsspørsmål og flere åpne spørsmål. Her fikk jeg se nytten av å ha utformet en intervjuguide med refleksjonsspørsmål om temaer med mer strukturerte underspørsmål. Jeg måtte også jobbe aktivt med å oppsummere og spørre om jeg hadde forstått informantene riktig, i tillegg til å ta tak i informasjon som «forsvant i mengden» for å følge opp informasjonen. Mot slutten stilte jeg avrundingsspørsmål som også var relativt «ufarlige» spørsmål om forventninger til hvordan temaet og arbeidet med datakriminalitet kommer til å utvikle seg i tiden fremover, samt om informanten hadde noen innspill eller tanker rundt

forskningsprosjektet, avsluttende spørsmål eller lignende. Jeg informerte også om hva som ville skje med forskningsprosjektet videre og når prosjektet er planlagt avsluttet. Alle informantene bidro med veldig mye og god informasjon, noe jeg passet på å presisere for dem for å vise at jeg satte pris på deres bidrag og at de skulle få en positiv avslutning på intervjuet (Tjora, 2012, s. 112-114; Johannessen et al., 2020, s. 111-112).

Jeg gjorde meg mange verdifulle erfaringer fra prosessen med intervjuene. Jeg la ned mye jobb når det kom til å gi god informasjon til informantene slik at de skulle føle seg trygge. Videre måtte jeg ha en god struktur og oversikt over når de forskjellige intervjuene skulle finne sted, hvilke lydfiler som tilhørte intervjuene og hvilke intervjuer som ble transkribert underveis. Jeg gjennomførte intervjuene ved siden av en vanlig jobbhverdag noe som krevde god planlegging. Selv om jeg opplevde at alle informantene kom med god informasjon og at alle intervjuene bidro med nye perspektiver, merket jeg at intervjuene ble bedre og bedre ettersom jeg som intervjuer også fikk mer erfaring med intervjusituasjonen og med bruken av intervjuguiden min. Jeg opplevde den positive virkningen av å ha en semistrukturert tilnærming med strukturerte underspørsmål til temaene. Da jeg ble kjent med og trygg på intervjuguiden ble det enklere å veksle mellom tematikk på en enkel måte, noe som bidro til at intervjuene kunne utfolde seg som en vanlig dialog. Det jeg opplevde som mest utfordrende var å sikre at jeg hadde forstått informantene riktig. Jeg opplevde også etter flere intervjuer at mange av informantene kom med mye lik informasjon, men i forskjellige perspektiver og med bruk av ulike begreper og satt inn i forskjellig kontekst. Her opplevde jeg at det ble viktig å stille oppfølgende og oppklarende spørsmål som «er det riktig dersom jeg tolker det du sier nå som» og «så hvis jeg forstår deg riktig så snakker du nå om». Dette lettet arbeidet med å se mønstre både underveis i prosessen, hvor den abduktive tilnærmingen med veksling mellom data og teori kommer inn, samt med analysen i etterkant. Det var flere ganger da jeg hørte på lydfilene under transkriberingen og under koding og kategorisering at jeg var glad for at jeg stilte de oppklarende spørsmålene. Samtidig var det viktig å passe på at jeg ikke endret på informasjonen informantene kom med gjennom å pålegge det min tolkning, og at de opplevde at de kunne rette på min oppfattelse dersom den ikke var riktig. Samtidig som jeg fikk gått dypt inn sentral informasjonen var det flere ganger under transkriberingen og analysen at jeg tenkte at det var informasjon jeg kunne ha fulgt opp enda bedre.

3.3 Databehandling

I samfunnsforskning er det mennesker som studeres og det kan fort oppstå etiske spørsmål og dilemmaer. I forskning skal man følge lov om behandling av personopplysninger, personopplysningsloven. Dersom personene som deltar i undersøkelsen ikke kan identifiseres, verken direkte eller indirekte, anses personene som anonyme og omfattes ikke av personopplysningsloven. Da er det i utgangspunktet ikke nødvendig å melde inn prosjektet til Norsk senter for forskningsdata (NSD) (Johannessen et al., 2020, s. 47-49). Det var ikke mange personopplysninger jeg var avhengig av å innhente, men siden stilling og arbeidsgiver var sentrale momenter i utvelgelsen kunne de i ytterste konsekvens bli identifisert indirekte gjennom denne informasjonen. Jeg meldte derfor prosjektet til NSD for å ivareta kravene i personopplysningsloven, og prosjektet ble godkjent 19. november 2021 (se vedlegg 3).

Ifølge forvaltningsloven er all informasjon som kan tilbakeføres til enkeltpersoner taushetsbelagt. Derfor skal resultater fra prosjekter som inneholder personopplysninger formidles i anonymisert form (Johannessen et al., 2020, s. 50). Anonymiteten til informantene som deltok i mitt forskningsprosjekt ble ivaretatt gjennom bruk av pseudonymer. I tillegg bruker jeg bransjekategorier for virksomhetene eller organisasjonene de jobber for. Jeg forsikret meg innledningsvis i intervjuet at informantene forstod at de og deres virksomhet eller organisasjon ville bli anonymisert i formidlingen av dataene og funnene fra undersøkelsen min. Jeg opplevde at dette var viktig for mange da uttalelser om erfaringer, samarbeid og praksis fort kunne blitt vanskelig dersom denne informasjonen i senere tid kunne blitt knyttet til informantene. jeg opplevde likevel ærlige og gode intervjuer noe jeg tror baserte seg på et etablert tillitsforhold gjennom god informasjon og gode rutiner i forskningsarbeidet. Ingen av informantene har imidlertid hatt innvendinger mot hvordan empirien blir formidlet, bruk av pseudonymer eller bransjekategorier. Noe av informasjonen som kom frem i intervjuene kan enkelt spores tilbake til person og virksomhet. I de tilfellene hvor uttrekk fra intervjuer blir formidlet vil identifiserende informasjon endres slik at formidlingen holdes anonym. Tabell 3.1 viser en oversikt over informantene med pseudonymer, bransjekategori og tilhørighet til utvalg.

Pseudonym	**Bransjekategori**	**Utvalg**
Vibeke	Industri	Utvalg 1
Andreas	Teknologi og innovasjon	Utvalg 1
Ola	Import og salg	Utvalg 1
Ole Gunnar	Finans	Utvalg 1
Kåre	Matproduksjon	Utvalg 1

Karl	Transport	Utvalg 1
Tone	Media	Utvalg 1
Markus	Maritim logistikk	Utvalg 1
Stian	Teknologi og innovasjon	Utvalg 1
Erik	Eiendom	Utvalg 1
Pål	Industri	Utvalg 1
Sondre	Privat sikkerhetsselskap	Utvalg 2
Patrick	Privat sikkerhetsselskap	Utvalg 2
Bård	Politi- og lensmannsetaten	Utvalg 2
Thomas	Politi- og lensmannsetaten	Utvalg 2
Harald	Offentlig myndighetsorgan	Utvalg 2
Kristoffer	Politi- og lensmannsetaten	Utvalg 2
Ruben	Politi- og lensmannsetaten	Utvalg 2

Tabell 3.1 Oversikt over informantenes pseudonym, bransjekategori og tilhørighet til utvalg

Man kommer som regel langt med høflighet, respektfull oppførsel og en viss gjensidighet. Det er likevel viktig å tenke gjennom etiske dilemmaer og elementer fordi relasjonen mellom forskeren og informanten ikke er symmetrisk. Selv om deltakerne i forskningsprosjektet er informert samtykke og retten til når som helst kunne trekke seg, er det også mulig at mange tenker at de ikke ønsker å «svikte» noe som kan påvirke informasjonen de kommer med. Aspekter som tillit, konfidensialitet, respekt og gjensidighet vil prege relasjonen og informasjonen (Tjora, 2012, s. 39-41). Jeg var opptatt av å gjennomføre intervjuene på en respektfull måte hvor informantene ikke skulle føle seg presset til å komme med informasjon de ikke følte seg komfortable med. Jeg opplevde at jeg fikk til å skape en trygg situasjon med bakgrunn i at flere av informantene tok opp enkelte ting de ikke ønsket å gå inn på og vi ble enige tidlig i intervjuene hvordan de eventuelt kunne snakke om situasjoner eller erfaringer på en måte de følte seg komfortabel med. Der informantene kom med informasjon som de ikke ønsket at jeg skulle ta med eller bruke, men de ønsket likevel å nevne det til meg for at jeg skulle forstå, ble vi enige om at jeg utelater det. Å få til en åpen dialog hvor man kan bli enige om «spillereglene» for å få informasjon og forvalte denne informasjonen videre på en respektfull måte var en god erfaring når det kommer til å følge etiske hensyn i en forskingsprosess.

3.4 Dataanalysen

Den kvalitative analysen skal gjøre det mulig for en leser av forskningen å få økt kunnskap om saksområdet det forskes på uten å selv måtte lese gjennom dataene som er generert i

forskningsprosjektet. Når man jobber med kvalitative data er det ofte en fordel at den som har samlet inn dataene også bør analysere og tolke dem, noe jeg merket viktigheten av da jeg jobbet med dataene fra datainnsamlingen. Å høre på lydopptakene fra intervjuene og transkribere dem gjorde at jeg fikk forståelse og kunnskap som jeg tok med meg videre inn i arbeidet med analysen og fortolkningen (Tjora, 2012, s. 174; Johannessen et al., 2020, s. 155).

Kvalitative data taler ikke for seg selv, de må tolkes. Analyse og fortolkning glir gjerne over i hverandre, selv om analysen på mange måter starter samtidig med forskningsprosessen og er med oss gjennom hele prosjektet. Likevel er det noen forskjeller. Under analysen vil man se på elementer av det som kommer frem, altså deler av en større helhet. Hensikten med å jobbe med dataene på denne måten er å finne mønstre, mening og avdekke et budskap. Etter analysen trekkes det gjerne konklusjoner som skal svare på problemstillingen. Når vi tolker noe så setter vi det inn i en større sammenheng. Her vil målet være å finne mening som ikke nødvendigvis kommer frem i direkte form. I fortolkningen vil man gjerne se på funnene opp mot teori på området. På denne måten prøver man å forstå og forklare funnene (Nilssen, 2012, s. 101; Johannessen et al., 2020, s. 155-156). For forskningsprosessen min var det helt avgjørende at det var jeg som jobbet med dataene fra start til slutt. Jeg merket godt at analysen og fortolkningen skjedde vekselsvis gjennom arbeidet med dataene, noe som også var i tråd med den abduktive tilnærmingen i SDI-modellen.

3.4.1 Transkripsjon gjennomgang av innholdet fra intervjuene

Det finnes ingen objektiv oversettelse fra muntlig til skriftlig form, derfor kan det være lurt å være detaljert når man transkriberer intervjuer tatt på lyd. Det kan ofte være lurt å heller ta med noe man er usikker på om man trenger til analysen, for så å ta denne avgjørelsen når man har bedre oversikt over hva som er viktig. Det er mye vi ikke kan direkte «oversette» fra det muntlige til det skriftlige. Når vi snakker vil vi for eksempel ikke bruke tegn, og vi sier ikke at vi starter på et nytt avsnitt. Det som kanskje er det største tapet når vi transkriberer er det visuelle og informasjon om stemningen under intervjuet eller når viktig informasjon kommer frem. Man kan likevel vinne mye på å transkribere intervjuene selv fordi man kan settes tilbake i en intervjusituasjon man selv har vært en del av når man leser transkriberingen (Tjora, 2012, s. 144-145). Jeg tok intervjuene på lyd og måtte derfor transkribere materialet. Jeg forsøkte å transkribere intervjuene i nær tid etter at intervjuet var gjennomført da jeg fremdeles hadde stemningen fra intervjuet friskt i minnet, og jeg forsøkte å beskrive denne stemmingen i transkriberingen. Jeg transkriberte totalt 18 intervjuer som endte i ca. 120 sider

med tekst. Det var tidkrevende, samtidig som det var nyttig å høre intervjuet etter at det var gjennomført. Siden jeg jobbet etter en abduktiv metode fikk jeg generert nye tanker, spørsmål og forståelse underveis i arbeidet som gjorde meg nysgjerrig på å finne ut mer om nye elementer intervjuobjektene hadde bragt til bords. I denne sammenheng var det også nyttig å føre en forskerlogg med tanker og resonnementer. Jeg opplevde under transkriberingen at det var vanskelig å gjengi informasjonen på den samme måten som den kom frem. Jeg forsøkte likevel å gjøre dette ved å legge til kommentarer til meg selv som for eksempel «intervjuobjektet ler og virker litt oppgitt».

3.4.2 Koding og kategorisering

Etter transkriberingen og føringen av forskerlogg satt jeg igjen med det som kalles analysedata. I denne fasen var det svært vanskelig å se noen sammenheng i et stort og omfattende datamateriale. Det var for det videre arbeidet hensiktsmessig å ha all dataen i tekstform som jeg kunne kode i detalj. Koder er i denne sammenheng ord eller uttrykk som beskriver et avsnitt eller et enda mindre utsnitt av datamaterialet. Jeg gikk frem ved å lese nøye gjennom hvert intervju og finne koder gjennom å bruke begreper som fremkom i materialet eller å identifisere koder gjennom å tolke hva setningene og avsnittene betydde. Jeg startet med et intervju og skrev ned alle kodene jeg fant. Så fortsatte jeg til neste intervju og fortsatte med de samme kodene som fra det forrige intervjuet, og la til nye der jeg fant dem. Sånn fortsatte jeg gjennom alle intervjuene. Til slutt satt jeg igjen med en omfattende liste over koder som jeg genererte gjennom et induktivt utgangspunkt i analysedataene mine. Jeg fokuserte på å generere tekstnære koder, altså koder som kun var utviklet fra dataene jeg leste, ikke fra teori, hypoteser, forskningsspørsmål eller planlagte temaer, selv om det til tider var fristende da jeg begynte å se noen temaer gå igjen. På dette tidspunktet valgte jeg å stole på prosessen og metoden. Å jobbe med koding på denne måten er også i tråd med SDI-modellen (Tjora, 2012, s. 179-180). Kodesettet jeg satt igjen med dannet et godt grunnlag for den videre jobbingen med kategorisering.

Kategorisering består av å samle kodene som er relevant for problemstillingen i forskjellige grupper. På dette tidspunktet kunne jeg utelate flere av kodene fordi det ikke lenger var empirien som bestemte hva som var relevant, men problemstillingen og forskningsspørsmålene. Kategoriene vil presentere et utgangspunkt for hva vi vil ha som hovedtemaer i analysen (Tjora, 2012, s. 185-186). Jeg benyttet en tversnittbasert og kategorisk inndeling av datamaterialet. Det går ut på å finne en inndeling på tvers av

materialet. Tanken bak å bruke kategorisering er å benytte det samme settet med kategorier systematisk og konsekvent på hele datamaterialet. Kategoriene ble utformet med bakgrunn i kodesettet, min bakgrunnskunnskap om temaet, problemstillingen og ny innsikt etter å ha jobbet etter en abduktiv tilnærming hvor jeg tilegnet meg ny kunnskap gjennom teori underveis i prosessen. Jobben med koding og kategorisering var langt mer omfattende enn jeg hadde sett for meg og jeg måtte virkelig jobbe for å komme frem til de kategoriene og underkategoriene som jeg skulle benytte for hele datamengden. Likevel opplevde jeg denne omstendelige prosessen som givende fordi det hjalp meg å få en struktur i et overveldende datamateriale og jeg kunne endelig begynne å se konturene av oppgaven min (Johannessen et al., 2020, s. 157-159).

For arbeidet med kodene og kategoriseringen benyttet jeg programmet NVivo som er et dataprogram til bruk i kvalitativ analyse. Programmet bygger på en tversnittbasert datareduksjon og analyse og er et godt verktøy i arbeidet med å kode, analysere og fremstille kvalitativt forskningsmateriale (Johannessen et al., 2020, s. 165). Etter prosessen med koding og kategorisering endte jeg opp med 4 hovedkategorier med 10 underkategorier i første linje. Flere av underkategoriene har flere underkategorier igjen i andre linje. Tabell 3.1 viser en beskrivelse av kategoriene med underkategorier funnet ved datareduksjon.

Hovedkategori	**Hovedkategori 1** Politiet og datakriminalitet	**Hovedkategori 2** Virksomhetenes beredskapsarbeid	**Hovedkategori 3** Eksterne faktorer	**Hovedkategori 4** Datakriminalitetens natur
Underkategori første linje	• Politiets arbeid med datakriminalitet • Politiet, datakriminaliteten og de andre aktørene • Politiets eksterne kommunikasjon	• Viktigheten av gode forberedelser • Relasjon til politiet • Faktorer som påvirker vurderingene rundt samarbeid	• Media • Samfunnet	• Datakriminaliteten • De datakriminelle
Beskrivelse av hovedkategori og underkategorier	Denne hovedkategorien tar for seg hvordan politiet jobber med datakriminalitet, og hvordan dette spiller inn på samarbeidet med virksomhetene. Sentralt i underkategoriene ble politiets kapasitet og kompetanse, overlappende mandater med andre aktører, politiets synlighet i mediebildet og ekstern kommunikasjon til virksomhetene	Denne hovedkategorien tar for seg hvordan virksomhetene jobber med sikkerhet og beredskap, og hvordan dette arbeidet spiller inn på samarbeid med politiet når det kommer til datakriminalitet. Sentralt i underkategoriene ble ledelse, sikkerhetskultur, kunnskap og kompetanse, trening og øving, risikoforståelse og kommunikasjonsstrategi.	Denne hovedkategorien tar for seg hvordan eksterne faktorer (ikke politiet eller virksomhetene) kan påvirke samarbeidet mellom de norske virksomhetene og politiet når det kommer til forebygging og håndtering av datakriminalitet. Sentralt i underkategoriene ble medias fremstilling av virksomheter som har blitt utsatt for alvorlig datakriminalitet og hvordan samfunnets holdninger til digital sikkerhet kan påvirke samarbeidet.	Denne hovedkategorien tar for seg datakriminaliteten. Sentralt ble datakriminalitet som en grenseoverskridende form for kriminalitet og hvordan datakriminaliteten utfordrer politiet og virksomhetene. Datakriminaliteten utvikler seg raskt og skaper et hurtig skiftende trusselbilde. De datakriminelle er ofte svært profesjonelle

Tabell 3.2 Oversikt over kategorier og underkategorier (første linje) funnet ved analyse av transkripsjoner fra intervjuene

3.4.3 Litteratursøk og teori

Forskningsprosjektet har et teoretisk rammeverk, og teori og litteratur som brukes til å tolke eller forklare funnene. Alle studier vil ha et slikt rammeverk, og det vil ofte basere seg på forståelsen og holdningene som forskeren tar med seg inn i forskningsprosessen. Det teoretiske rammeverket vil påvirke alle deler av undersøkelsen, og det kan sammenlignes med en linse man ser gjennom. Gjennom analysen og tolkningen vil man pendle mellom teori og datamaterialet (Nilssen, 2012, s. 62 og s. 105). SDI-modellen er abduktiv gjennom at man veksler mellom en induktiv og deduktiv tilnærming til empiri og teori. Man jobbe fra rådata til konsepter eller teorier, og sjekke dette fra det mer teoretiske til det empiriske. SDI-modellen kan gi inntrykk av at forskningsprosessen er lineær, noe som ikke er tilfellet. I praksis vil man kunne være på forskjellige stadier i modellen samtidig (Tjora, 2012, s. 175). Med bakgrunn i min erfaring og utdanning innen beredskap og kriseledelse gjennom flere år hadde jeg kjennskap til en del sentrale teorier innen samfunnssikkerhet og beredskap som jeg anså relevante for forskningsprosjektet. I forberedelsesfasen jobbet jeg mye med å finne tema og ikke minst spisse tema og vinkling. Gjennom dette arbeidet gjorde jeg søk etter relevant teori og litteratur og leste meg opp. Siden jeg jobbet ut fra SDI-modellen gjorde jeg også litteratursøk underveis i forskningsprosessen ettersom jeg gjennomførte intervjuer og oppdaget nye funn og perspektiver og jobbet med koding og kategorisering av datamaterialet. Denne prosessen resulterte også i at jeg endret problemstillingen min flere ganger ettersom jeg fikk mer kunnskap og klarte å spisse det enda mer inn mot fenomenet jeg undersøkte. Den endelige problemstillingen og forskningsspørsmålene var ikke ferdigstilt før jeg hadde gått gjennom den største delen av materialet fra datainnsamlingen. På dette tidspunktet så jeg at funnene i et overordnet perspektiv dreide seg om hvordan politiets arbeid med datakriminalitet og virksomhetenes beredskapsarbeid påvirket hverandre i samarbeidet med forebygging og håndtering av datakriminalitet.

Mye av teorien og litteraturen som jeg tenkte at jeg kom til å ta utgangspunkt i før jeg startet arbeidet med datainnsamlingen viste seg å ikke være like relevant ettersom jeg arbeidet med datamaterialet og fikk nye perspektiver og forståelse for tematikken. Samtidig kom ny teori og litteratur til ettersom jeg jobbet meg gjennom materialet. Dette dreide seg i all hovedsak om sentral teori innen samfunnssikkerhet og beredskap, samt offentlige dokumenter som omhandlet tematikken. Jeg gjorde også søk etter nyere forskning på området, noe jeg opplevde som utfordrende. Jeg ba derfor om en time med Nord Universitet sitt bibliotek. Jeg

fikk rask respons og hadde en lærerik og nyttig time digitalt med en av de ansatte ved biblioteket som ga meg gode tips og råd for hvordan jeg kunne gå frem da jeg skulle søke etter litteratur. Databasene jeg brukte i mine søk var Google Scholar, Oria, PIA og Idunn. Søkeordene jeg brukte var ord som cybercrime, police handling cybercrime, underreporting cybercrime, law enforcement, cybercrime prevention, digital threats, information security, cyber security culture, business victimization. Jobben med litteratursøk var utfordrende og det var vanskelig å finne forskning på området, noe som kan skyldes at det ikke eksisterer så mye forskning på området enda og at tematikken jeg har valgt for oppgaven er en relativt «ny». I tillegg er forholdet mellom virksomheter og politiet varierende rundt om i verden. Jeg fant likevel noe forskning fra andre land som traff tematikken godt. I tillegg benytter jeg offentlige dokumenter. Et godt tips jeg fikk av biblioteket ved universitetet var å se på referanselistene til andre masteroppgaver med lignende tematikk. Jeg spurte også informantene på slutten av intervjuet om de hadde noen tanker om litteratur som kunne være aktuell for oppgaven min. Det teoretiske rammeverket for oppgaven baserer seg i all hovedsak på kjente teorier fra fagfeltet samfunnssikkerhet og beredskap som har vært sentrale i løpet av masterstudiet og offentlige dokumenter som omhandler digital sikkerhet.

3.5 Pålitelighet, validitet og generalisering

Innen kvalitativ forskning benyttes gjerne tre forskjellige kvalitetskriterier som indikatorer for kvalitet i forskningen. De tre kriteriene kalles pålitelighet, som handler om intern logikk gjennom forskningsprosessen, validitet som handler om logisk sammenheng mellom prosjektets utforming, funn og de spørsmålene man søker å besvare, og generalisering som er knyttet til forskningens gyldighetsområde utover de enheter som faktisk er undersøkt (Tjora, 2012, s. 202).

Når man skal gjennomføre et forskningsprosjekt er det enkelt å velge et tema man engasjerer seg i og som man har forkunnskaper om. Å være nøytral eller fullstendig objektiv til det man undersøker kan omtales som et ideal, men det er sjeldent mulig å være fullstendig nøytral. De forkunnskapene og den forforståelsen man møter et prosjekt med vil kunne være fordelaktig. Samtidig er det viktig å være bevisst hvordan ens egen posisjon kan påvirke forskningsarbeidet fordi det er menneskelig å være mer åpen for funn som støtter det vi tror, noe som kan gjøre at vi overser informasjon som ikke «passer inn» i mønsteret man selv ser. Dette kan redusere påliteligheten av forskningsresultatene dersom vi ikke er bevisst det og ikke tørr å være åpen for å også å se etter informasjon som er motstridene med våre tanker,

holdninger og meninger om et fenomen (Tjora, 2012, s. 203; Nilssen, 2012, s. 139). Påliteligheten kan styrkes ved å gi leseren inngående beskrivelser av konteksten, og være åpen og detaljert i fremstillingen av fremgangsmåten under hele forskningsprosessen. For å ivareta påliteligheten i min forskningsprosess har jeg beskrevet de valgene jeg har tatt, metodene jeg har jobbet etter, hvordan jeg har samlet inn data og jobbet med disse gjennom datareduksjon og kategorisering, og jeg har forsøkt å legge frem vurderinger og tanker jeg har hatt underveis i prosjektet. Videre har det vært viktig for meg å være bevisst mitt eget faglige ståsted og utgangspunkt. Jeg har funnet stor hjelp i å «stole på prosessen» og ikke ta fristende snarveier eller hoppe til konklusjoner basert på hva min kunnskap og erfaring tilsier. Dette var også noe av bakgrunnen for at jeg valgte å ha to intervjuutvalg, hvor det ene utvalget bestod av mennesker som har et relativt likt utgangspunktet og kunnskapsgrunnlag som meg selv. Dette gjorde det enklere for meg å innta en mer objektiv rolle i forskningsprosessen, samtidig som jeg også fikk utfordret min forforståelse (Johannessen et al., 2020, s. 250).

Validitet handler om hvorvidt funnene fra undersøkelsen faktisk er svar på de spørsmålene som stilles. Data kan ses på som representasjoner av virkeligheten og da blir spørsmålet hvor godt eller relevant data representerer det fenomenet vi forsker på. Dette kalles gjerne intern validitet. I kvalitativ forskning må forskeren forsikre leseren om at det bildet som males ikke er en forvrengning av de faktiske forhold. Funnene må være konsistente med datamaterialet som ble samlet inn. Fordi vi mennesker har forskjellige utgangspunkt, kunnskap og perspektiver vil heller ikke en kvalitativ studie kunne gjennomføres helt likt en gang til. For å ivareta den interne validiteten i min undersøkelse benyttet jeg to teknikker som øker sannsynligheten for at forskningen frembringer troverdige resultater. Jeg brukte teknikken vedvarende observasjon gjennom å investere mye tid i å sette meg godt inn i feltet og tematikken slik at jeg enklere kunne skille mellom relevant og ikke-relevant informasjon. Videre brukte jeg teknikken metodetriangulering gjennom å ta utgangspunkt i flere settinger eller caser, gjennom å intervjue personer fra forskjellige virksomheter og organisasjoner. Jeg kunne ha styrket troverdigheten ytterligere gjennom å tilbakeføre resultatene til informantene for å bekrefte resultatene, eller ved å la andre kompetente personer analysere det samme datamaterialet for å sjekke konsensus. Dette hadde både vært nyttig og interessant dersom jeg i min masteroppgave hadde hatt tid og ressurser til å gjennomføre en slik prosess (Johannessen et al., 2020, s. 43 og s, 250; Tjora, 2012, s. 206-207; Nilssen, 2012, s. 141).

Generalisering dreier seg om overførbarhet og om resultatene fra undersøkelsen kan overføres til liknende fenomener, gjennom å etablere beskrivelser, begreper, fortolkninger og

forklaringer som er nyttige på andre områder enn det som studeres. I kvalitativ forskning baserer datainnsamlingen seg gjerne på noen få individer som har visse felles egenskaper, og vi går i dybde i stedet for bredde. På denne måte kan man se på resultater fra kvalitative undersøkelser som kontekstuelt unike. Studiets generalisering styrkes dermed gjennom fyldige beskrivelser av detaljer som inngår i et fenomen. Jeg valgte dybdeintervjuer i min studie, noe som ville kunne gjøre det enklere for andre å bedømme om studiens resultater kan overføres til andre kontekster (Johannessen et al., 2020, s. 251-252). Gjennom arbeidet med systematisering og analyse av datamaterialet plukket jeg helheten fra hverandre og bygget dette opp igjen gjennom en ny og «forskerkonstruert» kunnskap om fenomenet etter bearbeiding av materialet sett opp mot teori på området og sammenstilling av informasjon. Dette kan ses på som et forenklet, men typisk bilde av den opprinnelige virkeligheten. Jobben med dette lå i å tolke materialet gjennom de funnene som kom frem, min bakgrunnskunnskap om fenomenet og relevant teori og litteratur på området. Det handlet om å trekke slutninger ut over de umiddelbare opplysningene som jeg samlet inn (Johannessen et al., 2020, s. 251).

Vi kan si at målet med kvalitativ forskning er å utvikle innsikt knyttet til et bestemt fenomen, hvor denne innsikten kan testes i form av en konsept- eller teoriutvikling. Ifølge SDI-modellen er konseptuell generalisering målet. Her er man ute etter å fremstille funn i form av typologier, modeller, begreper, metaforer eller lovmessigheter som ikke direkte er knyttet til spesifikt kun til den empirien eller casen som ligger til grunn. For å sikre relevans utover de data som er analysert i prosjektet, benyttes tidligere forskning og teorier som støtter opp under en større gyldighet og generaliserbarhet (Tjora, 20212, s. 215). Gjennom å intervjue personer i forskjellige store norske virksomheter og personer fra politi- og lensmannsetaten, offentlig myndighetsorganer og private sikkerhetsselskaper og sammenligne svarene de ga i intervjuene, håpet jeg at dette kunne lede til at jeg fant mønstre, sammenfallende og motstridende informasjon som kunne bidra til å dra slutninger som gjelder på tvers av bransjer og «sider» av fenomenet. Styrken i dette ville ligge i å få uavhengige uttalelser fra personer med relativt like ansvarsområder og posisjoner, men med ulik bakgrunn, erfaringer og perspektiver. I tillegg så jeg funnene opp mot relevant teori innen fagområdet og nyere forskning, noe som vil kunne støtte oppunder funnene mine og gi de større gyldighet og generaliserbarhet. Noe av formålet med forskningsprosjektet var å få innsikt i fenomenet samarbeid mellom virksomheter og politiet når det kommer til datakriminalitet, og at denne innsikten og kunnskapen kunne deles videre med relevante virksomheter, nettverk og deler av politiet for å styrke et viktig samarbeid videre.

Å jobbe med forskningsprosjektet har vært en spennende oppgave med bratt læringskurve. Selv om mye av jobben har gått ut på å gjøre veloverveide valg når det kommer til metode, design og fremgangsmåte, lå også en del av jobben i det å være bevisst kilder til feil som kunne oppstå i løpet av prosessen. Et eksempel på en slik feilkilde nevnte jeg i avsnittet over når det gjaldt det å ikke bare se data og funn som stemte overens med mine egne tanker, holdninger og antakelser om fenomenet, men også informasjon og funn som strider med mine antakelser. Det finnes flere slike feilkilder som man som forsker kan møte på i en forskningsprosess. Når man gjennomføreren kvalitativ studie og benytter intervju som kilde til data kan nærhetsprinsippet utfordre forskningens troverdighet. I en kvalitativ studie kan man oppleve å ha en dobbeltrolle gjennom at man gjerne er forsker i sin egen kontekst og med det innehar «innsidekunnskap» om fenomenet. Med min bakgrunn vil jeg nødvendigvis inneha en del kunnskap utover det datamaterialet gir. Denne kontekstkunnskapen kan på den ene siden være positiv i et tolkningsarbeid, samtidig som denne nærheten til fenomenet også kan utfordre «forskersynet». Det var derfor viktig å klare å holde en viss distanse til forskningsdeltakerne, konteksten og datamaterialet (Nilssen, 2012, s. 137-138). Relativt tidlig i prosessen med intervjuer fikk jeg en opplevelse med dette ved at en av mine antakelser om fenomenet ble motbevist gjennom informasjonen fra flere av intervjuobjektene. Dette var på den ene siden utfordrende fordi det nettopp spilte på mine menneskelige egenskaper og et ønske om å finne informasjon som bekreftet mine antakelser og hypoteser, samtidig som det var fin læring tidlig i intervjuprosessen. Dette gjorde at jeg i større grad klarte å være bevisst denne kilden til feil og klarte å innta en mer objektiv tilnærming til informasjonen som fremkom i de følgende intervjuene. Gjennom denne prosessen gjorde jeg verdifull læring når det kommer til å være kritisk til eget forskningsarbeid.

3.6 Refleksjon over forskerrollen

I samfunnsvitenskapelig forskning vil påvirkningen mellom fenomen og forsker gå begge veier gjennom at forskeren selv er en del av det sosiale livet som er gjenstand for undersøkelse. Refleksiviteten, eller vekselvirkningen mellom forsker og fenomen, kan utspille seg i forskjellige former. Min tilstedeværelse som forsker påvirket situasjonen og også informantene, deres atferd og informasjonen de kom med. I tillegg ville min forforståelse av fenomenet påvirke hvordan jeg møtte forskningsprosessen, eksempelvis gjennom hvordan jeg formulerte spørsmålene i intervjuguiden, hvordan jeg stilte spørsmålene og hvem jeg valgte ut som informanter. Som nevnt er også en vanlig menneskelig egenskap å se etter den informasjonen som bekrefter våre holdninger, meninger og antakelser om et fenomen.

Forskningsprosjektet mitt er en del av både det fagfeltet masterstudiet dreier seg om i tillegg til at det er en sentral del av arbeidshverdagen min og noe jeg interesserer meg for. Bevissthet rundt refleksiviteten i forskningsprosessen min har derfor vært helt sentral, og en redegjørelse av forforståelsen helt nødvendig (Nilssen, 2012, s. 31; Tjora, 2012, s. 203; Johannessen et al., 2020, s. 26).

Det ble viktig for meg å identifisere hvilke grunnleggende antakelser jeg hadde om fenomenet før jeg startet arbeidet med intervjuguide, gjennomføring av intervjuene og analyse- og tolkningsprosessen. Måten jeg gjorde dette på var å stille meg selv spørsmålene fra intervjuguiden før jeg skrev ned antakelser og hypoteser om fenomenet. Erfaringer fra egen arbeidsplass, innhold i offentlige dokumenter og rapporter om datakriminalitet og saker om tematikken i mediebildet viser at det fremdeles er en vei å gå når det kommer til politiets arbeid med datakriminalitet og utnyttelse av potensialet som ligger i samarbeid mellom norske virksomheter og politiet for å forebygge og håndtere datakriminalitet. Jeg identifiserte mine egne tanker og forklaringer på hvorfor det er slik for å være bevisst dette inn i en prosess med datainnsamling og analyse. Det betydde ikke at jeg skulle se bort fra funn som var sammenfallende med mine antakelser og meninger, men at jeg skulle være forsiktig med å vektlegge disse funnene tyngre enn funn som var inkonsistente med mine egne antakelser og tørre å utfordre meg selv slik at jeg ikke ble blind på denne informasjonen. Videre var det viktig at jeg møtte intervjuobjektene på en nøytral måte og ikke lot mine holdninger og antakelser smitte over på dem gjennom min atferd, spørsmålsstilling og spørsmål. Dette ledet til at jeg endret litt på hvordan jeg stilte spørsmål underveis da jeg opplevde at noen av spørsmålene kunne oppfattes som ledende eller formulert på en måte som påvirket informantens oppfattelse av hva jeg var ute etter og på den måten hvilket svar de ga.

Det er viktig at funnene som presenteres i en studie er et resultat av forskningen og ikke av forskerens subjektive holdninger. I denne sammenheng er det viktig å beskrive alle beslutninger forskningsprosessen slik at leseren kan følge og vurdere disse beslutningene. Gjennom studien har jeg lagt vekt på å være selvkritisk til hvordan jeg skal gjennomføre de forskjellige fasene og opp mot vurderingene og beslutningene jeg har tatt. Dette har kanskje vært noe av det mest utfordrende, men også det mest lærerike gjennom forskningsprosjektet, nettopp å stoppe opp og bruke tid på å gjøre nøye vurderinger og være kritisk til de valgene jeg har tatt underveis (Johannessen et al., 2020, s. 252-253).

3.7 Kritisk refleksjon over forskningsdesign og metode

All samfunnsforskning dreier seg om å undersøke menneskers virkelighet, en virkelighet som består av uendelig med erfaringer, opplevelser, kunnskap, samhandling og fortolkninger. Det vil alltid være mulig å stille spørsmål ved de valgene man gjør som forsker når det kommer til valg av fremgangsmåter for en undersøkelse. Selv om jeg har gjort veloverveide valg og anser den fremgangsmåten jeg har gått for som å være den beste for mitt forskningsprosjekt, vil det eksistere svakheter og andre alternative fremgangsmåter som også ville kunne fungert godt (Johannessen et al., 2020, s. 25).

I en casestudie kan man med fordel benytte både kvantitative og kvalitative metoder for datainnsamling. En kombinasjon av disse metodene vil kunne gi mye og detaljerte data. Å kombinere kvantitative og kvalitative metoder ville kunne beriket dataene i undersøkelsen min. Samtidig ville dette vært svært tid- og ressurskrevende. En masteroppgave begrenser både tid og ressurser, og jeg ser at en slik tilnærming ikke hadde vært gjennomførbar med tiden jeg hadde til rådighet. Det kan tenkes at en ren kvantitativ tilnærming gjennom for eksempel en spørreundersøkelse også kunne gitt god informasjon som ville besvart problemstillingen min. Jeg ville her også hatt anledningen til å komme i kontakt med flere informanter noe som kunne styrket generaliserbarheten. Samtidig hadde det ikke gitt meg muligheten til å gå i dybden både gjennom utfyllende svar og oppfølgingsspørsmål, noe som har gitt meg god forståelse og innsikt i fenomenet (Johannessen et al., 2020, s. 212).

Utviklingen på området jeg valgte som tema i mitt forskningsprosjekt er et felt som er i stadig endring, både fra myndighetenes og virksomhetenes side. Med bakgrunn i den tiden man har til rådighet for å skrive en masteroppgave og gjennomføre forskningsprosjektet ble det naturlig å gjennomføre en tverrsnittsundersøkelse. Ved å gjennomføre en slik undersøkelse vi funnene kunne si noe om fenomenets tilstand på et gitt tidspunkt. Man kan også gjennomføre undersøkelser som strekker seg over tid, kalt longitudinelle undersøkelser. Ved å gjennomføre en tverrsnittsundersøkelse vil jeg ikke ha den samme muligheten til å avdekke årsakssammenhenger og utvikling over tid. Samtidig vil tolkningsprosessen kreve at jeg setter meg inn i utviklingen på området, og flere av informantene fant det naturlig å fortelle om sine erfaringer fra den tiden de har jobbet med tematikken, og jeg fikk på den måten ett innblikk i utviklingen og opplevelsen av fenomenet før og nå (Johannessen et al., 2020, s. 55).

I utvalget av informanter i kvalitative undersøkelser er det viktig å snakke med informanter som har mye og relevant informasjon om fenomenet som skal undersøkes.

Målgruppen jeg ønsket informanter fra baserte seg på det forberedende arbeidet med problemstilling og vinkling på temaet. Siden jeg var prisgitt at personer fra store norske virksomheter frivillig ville delta i undersøkelsen, måtte jeg være nøye med å beskrive kriteriene for de personene jeg ønsket å komme i kontakt med når jeg sendte henvendelser til virksomhetene. Jeg beskrev at jeg ønsket å komme i kontakt med personer som jobber med sikkerhet, herunder digital sikkerhet, og som hadde en sentral rolle i beslutningen til en virksomhet om å kontakte og samarbeide med politiet når det kommer til forebygging og håndtering av datakriminalitet. Basert på dette hadde jeg liten kontroll med akkurat hvilken rolle, stilling, erfaring eller bakgrunn mine informanter i utvalg 1 ville ha, og jeg måtte ha tillit til at virksomhetene klarte å finne gode informanter basert på inngangsverdiene. Jeg var usikker på hvorvidt denne tilnærmingen ville sette meg i kontakt med informanter som hadde mye og relevant informasjon om fenomenet. Jeg forstod raskt etter at jeg begynte med intervjuene at jeg hadde truffet godt med informasjonen jeg ga virksomhetene. Likevel var dette et moment som raskt kunne ha slått ut feil dersom ikke virksomhetene hadde forstått hvem jeg var ute etter å snakke med. I en kvantitativ undersøkelse trekkes utvalget ofte tilfeldig for å kunne gjøre statistiske generaliseringer basert på teorien om at et utvalg skal kunne representere den populasjonen det er trukket fra. Det er ikke vanlig og ofte lite aktuelt med en slik tilfeldig tilnærming til utvalg av informanter i kvalitative undersøkelser. Da jeg ikke visste hvem jeg kom til å komme i kontakt med følte jeg på et element av tilfeldighet, samtidig som jeg hadde forsøkt å motvirke et tilfeldig utvalg gjennom å gi nøye beskrivelse av kriterier. Jeg fikk god hjelp med utformingen av denne informasjonen gjennom å definere mine analyseenheter som hadde nær sammenheng med problemstillingen (Johannessen et al., 2020, s. 57-58 og s. 214).

Dersom jeg hadde hatt tilgang til å observere situasjoner i virksomhetene hvor myndighetskontakt og datakriminalitet ble diskutert hadde dette utvilsomt vært en spennende måte å samle inn data til forskningsprosjektet mitt på. I en slik situasjon ville jeg kunne fått tilgang på informasjon som ikke informantene hadde tolket selv før jeg fikk den, noe som er tilfellet i intervjuer. Det kunne vært mulig å gjennomføre observasjon som datainnsamlingsmetode, men det hadde krevd at jeg var tilgjengelig for å kunne møte opp for observasjon når de riktige situasjonene skjedde, for eksempel når en virksomhet blir utsatt for et dataangrep og prosessen skjer rundt hendelseshåndtering, eller når virksomheten driver beredskapsarbeid gjennom forskjellige beredskapsanalyser og forberedelser som for eksempel gjennomføringen av en øvelse. Også her kommer tid inn som en faktor som har spilt inn på

valgene jeg har tatt. Selv om dette hadde vært en spennende måte å samle inn data på var likevel intervju en datainnsamlingsmetodikk jeg anså som svært relevant for å forstå fenomenet da jeg ville ha større mulighet til å stille spørsmål og få inngående og detaljert informasjon om informantenes erfaringer, refleksjoner, meninger og opplevelser (Tjora, 2012, s. 46 og s. 105; (Johannessen et al., 2020, s. 79 og s.106).

Jeg valgte å utforme en semistrukturert intervjuguide med overordnede temaer og åpne spørsmål. Hensikten med dette var å åpne for muligheten for å veksle mellom temaer og «tilpasse» spørsmålsstillingen til intervjusituasjonen, samtidig som det skulle være en viss grad av struktur i det. Det første utkastet til intervjuguide ble imidlertid veldig åpen og generell, selv om den var temaspesifikk. Etter å ha gjennomført noen intervjuer så jeg raskt at alle intervjuene ville bli ganske forskjellige selv om vi var innom de samme temaene. Jeg opplevde også at jeg måtte klare å tilpasse intervjuet til hver informant. Med bakgrunn i dette endret jeg og spisset intervjuguiden slik at den som et utgangspunkt var semistrukturert med stor grad av fleksibilitet og åpenhet, samtidig som jeg la til spesifikke spørsmål under de forskjellige temaene som hadde et mer strukturert preg. Dette var til god hjelp når det kom til å tilpasse spørsmålene til hvert intervjuobjekt for å få mest mulig informasjon ut av informanten. Det kan argumenteres for at å ha en mer strukturert intervjuguide og tilnærming fra start av og gjennom alle intervjuene ville hjulpet i arbeidet med å sammenligne informasjon og svar. Samtidig tror jeg dette hadde blitt utfordrende å gjennomføre og at det hadde kunnet virke negativt med tanke på informasjonsflyten i intervjuene da informantene hadde forskjellige erfaringer, kunnskap, stilling, rolle, bakgrunn og opplevelse av tematikken (Johannessen et al., 2020, s. 107-109).

Intervjuguiden kan brukes som utgangspunkt for en fortløpende kategorisk inndeling av datamaterialet ved å sortere og kategorisere alle data fra alle informantene under hvert hovedtema. Denne måten å kategorisere på fungerer ikke alltid like godt da man fort kan ende opp med altfor brede kategorier eller forhåndsdefinerte kategorier som ikke bidrar med mye ny kunnskap. Det egner seg heller ikke for å fange opp ikke-tekstbaserte data og data som er samlet inn uten en fast struktur. Forskeren trenger derfor også andre verktøyer for å finne mønstre i datamaterialet. Her kan man bruke koding der man vil ende opp med flere kategorier som kan brukes på samme tekst og flere nivåer av kategorier og underkategorier (Johannessen et al., 2020, s. 159). Selv om kategoriene jeg endte opp med har en viss sammenheng eller likhet med strukturen i intervjuguiden er de et resultat av jobben som er gjort med koding og kategorisering, og ikke noe jeg hadde bestemt meg for på forhånd. Dette

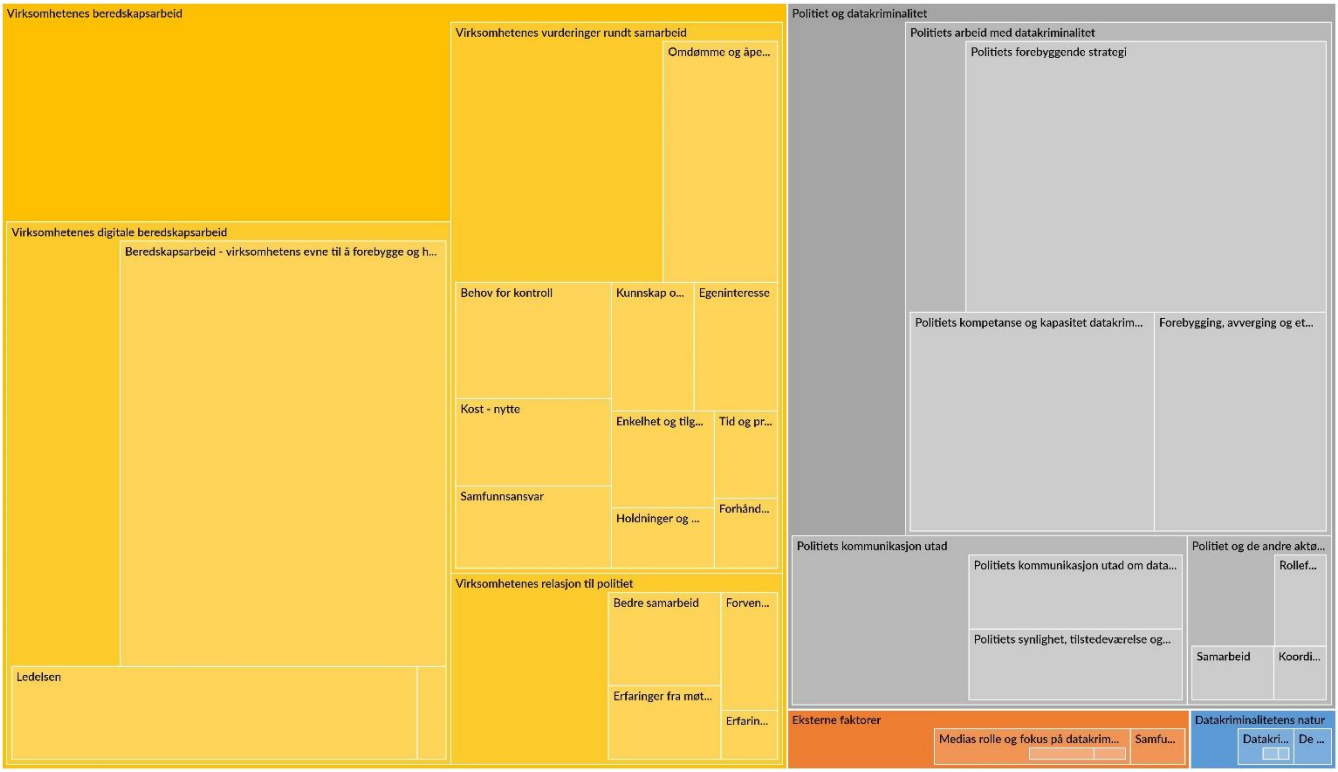
gjelder kanskje spesielt underkategoriene. Det var fristende på et punkt å etablere kategoriene tidlig i prosessen med koding og kategorisering da jeg hadde fått et visst inntrykk gjennom intervjuene, samtidig hadde jeg bestemt meg for å stole på prosessen, noe jeg var glad for at jeg gjorde da jeg så at kategoriene ble annerledes og bedre etter at jeg jobbet systematisk med kodingen og kategoriseringen.

3.8 Etiske betraktninger

En etisk sans bør ligge implisitt i all forskning. Dette dreier seg om aspekter som tillit, konfidensialitet, respekt og gjensidighet. Det vil oppstå en helt naturlig forventning om at man som forsker «gir noe tilbake» til de som frivillig deltar i forskningsprosjektet. I arbeidet med å finne informanter til intervjuene var jeg i starten usikker på hva jeg kunne forvente når det kom til respons og tilgjengelighet. Jeg ble positivt overrasket over hvor villige og positive informantene var til å delta og dele av sine erfaringer og opplevelser. Informasjonsskrivet jeg sendte ut ga informantene informasjon om hvordan deres personopplysninger ville bli behandlet, samt deres rettigheter til å trekke samtykket og sin deltakelse når som helst. Selv om jeg møtte på en villighet til å dele informasjon og delta forstod jeg også raskt at mye av dette baserte seg på informasjonen de hadde fått og at jeg var nøye med å holde tiden og informere underveis, både før, under og etter intervjuet om forskningsprosessen. Alle informantene hadde forskjellige behov når det kom til å vite hva som ville skje videre, hvordan informasjonen ville bli fremstilt og når de kunne forvente seg å se et resultat. Jeg var veldig takknemlig for at informantene var så på tilbudssiden som de var, og jeg merket godt at dette gjorde meg opptatt av å gjennomføre forskningsprosjektet på en måte som de var komfortable med. Hvordan jeg informerte informantene, hvordan jeg fremstod i intervjuene og hvordan jeg behandlet informasjonen som kom frem i tillegg til personopplysningene hadde mye å si for det tillitsforholdet som ble etablert, noe som igjen påvirket informasjonen informantene kom med (Tjora, 2012, s. 41). Flere momenter for etiske problemstillinger er gjort rede for under punkt 3.3.

4 Empiriske funn

Etter datagenereringen fulgte en omfattende prosess med koding og kategorisering. Jeg endte opp med 4 hovedkategorier og 10 underkategorier (første linje). Flere av underkategoriene hadde igjen underkategorier (andre linje). Det er hovedkategoriene og underkategoriene (første linje) som i all hovedsak vil bli presentert i dette kapitlet. Likevel vil noen av underkategoriene fra andre linje bli presentert der det er hensiktsmessig. Figur 4.1 viser en oversikt over det kodede materialet.



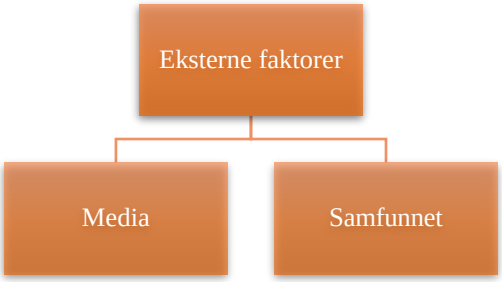
Figur 4.1 Oversikt over hovedkategorier og underkategorier i datamaterialet. Hentet fra NVivo.

I arbeidet med kodningen benyttet jeg analyseprogrammet NVivo. Figur 4.1 viser omfanget av datamaterialet og dybden i analysen gjennom hoved- og underkategorier. Årsaken til størrelsesforskjellen på de forskjellige kategoriene er at visualiseringen av kodingen baserer seg på funn knyttet til de forskjellige kategoriene. Hovedkategori 1 og 2 er størst da disse kategoriene omfatter hovedtyngden av funnene i datamaterialet. Hovedkategori 1 «Politiet og datakriminalitet» og hovedkategori 2 «Virksomhetenes beredskapsarbeid» vil bli presentert hver for seg. Hovedkategori 3 «Eksterne faktorer» og hovedkategori 4 «Datakriminalitetens natur» vil bli presentert under ett underkapittel, da disse hovedkategoriene ikke er like store når det kommer til innhold, og informasjonen som kommer frem er relativt overlappende. Figurene under viser hovedkategoriene med

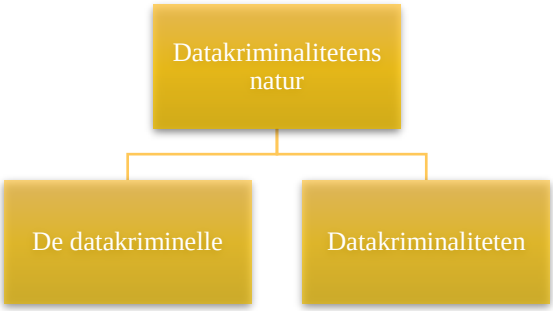
underkategorier (første linje) for å gi en oversikt over materialet som videre vil bli presentert i dette kapitlet.

Figur 4.2 Hovedkategori 1 – Politiet og datakriminalitet - med underkategorier (første linje)

Figur 4.3 Hovedkategori 2 – Virksomhetenes beredskapsarbeid – med underkategorier (første linje)



Figur 4.4 Hovedkategori 3 – Eksterne faktorer – med underkategorier (første linje)



Figur 4.5 Hovedkategori 4 – Datakriminalitetens natur – med underkategorier (første linje)

Videre vil jeg fremstille de empiriske funnene som tilhører hovedkategoriene. Jeg vil under hver hovedkategori presentere underkategoriene (første linje) med deres respektive

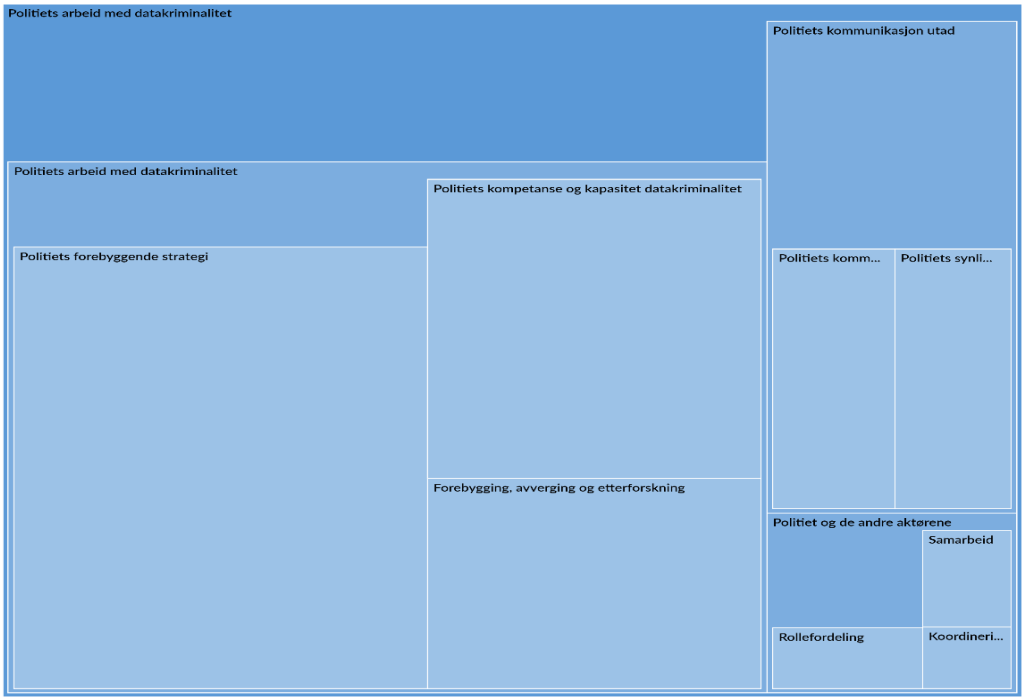
underkategorier i andre linje, der det er hensiktsmessig. Følgende vil bli presentert videre i fremstillingen av empirien:

- **4.1** Politiet og datakriminalitet
- **4.2** Virksomhetenes beredskapsarbeid
- **4.3** Datakriminalitet, media og samfunnet

I dette kapitlet er hensikten å fremstille mine funn for å gi et innblikk i hva som har kommet frem gjennom datainnsamlingen i undersøkelsen. Empiriske utdrag vil bli brukt for å illustrere mangfoldet i datamaterialet. Sitatene fra informantene vil merkes med pseudonym og bransje. Jeg gjennomførte totalt 18 intervjuer i to forskjellige intervjuutvalg. En nærmere beskrivelse av disse utvalgene finnes i kapittel 3. For å ivareta informantenes anonyme deltakelse i undersøkelsen har hver informant fått et pseudonym. I tillegg har de blitt knyttet til en bransjekategori slik at også deres arbeidsgiver blir anonymisert. Informantene i utvalg 2 som er knyttet til politi- og lensmannsetaten har bekreftet at de er komfortable med å knyttes til denne bransjekategorien. De er ansatt forskjellige steder i politi- og lensmannsetaten. En oversikt over informantenes pseudonym, bransjekategori og tilhørighet til utvalg finnes i tabell 3.1 i kapittel 3.

4.1 Politiet og datakriminalitet

I dette underkapitlet presenteres hovedkategori 1 «Politiet og datakriminalitet». Figur 4.6 viser en fremstilling av hovedkategorien med underkategorier.



Figur 4.6 Oversikt over hovedkategori 1 – Politiets arbeid med datakriminalitet. Hentet fra NVivo

Jeg vil videre gå nærmere inn på de forskjellige underkategoriene i første linje og deres underkategorier i andre linje der det er hensiktsmessig. Politiet og datakriminalitet var et tema som ble sentralt i alle intervjuene. De to intervjuutvalgene hadde både sammenfallende og inkonsistente oppfattelser, erfaringer, kunnskap om og opplevelser når det kom til politiets arbeid med datakriminalitet.

4.1.1 Politiets kompetanse, kapasitet og tillitsskapende arbeid

De fleste informantene i utvalg 2 mener at politiet har kommet for sent på banen når det kommer til å forebygge og håndtere datakriminalitet, og at politiet generelt henger bak når det kommer til kompetanse på området. Datakriminalitet har ikke blitt prioritert tilstrekkelig av politiet, og kapasiteten til å håndtere denne kriminalitetsformen oppleves som mangelfull. Informanter fra begge utvalgene mener at manglende kompetanse og kapasiteten hos politiet kan ha ført til at andre aktører, både offentlige og private, har kommet på banen og tatt plass på en arena hvor politiet bør ha kontroll.

> Jeg tror at politiet har kommet alt for sent i gang med dette fagområdet. Man har jo jobbet med datakriminalitet i politiet lenge, helt tilbake til da man opprettet en avdeling for dette i Økokrim på 90- tallet en gang, men det har jo aldri fått det fokuset og den prioriteringen det trenger, kanskje ikke før nå med opprettelsen av NC3. Det er over veldig mange år folk som har gjort en god jobb med dette i politiet, men de har vært konstant underbemannet og underfinansiert. Jeg tror dette har ført til at andre aktører, og dette er ikke unikt for Norge, har fått muligheten til å ta det rommet som politiet egentlig burde hatt (Sondre, Privat sikkerhetsselskap).

De fleste av informantene i utvalg 1 opplever at politiet ikke har klart å etablere en struktur som gjør det enkelt for dem å anmelde og dele informasjon om datakriminalitet med politiet. I tillegg forteller flere av dem at de er usikre på hvordan politiet jobber med datakriminalitet og hvilken kompetanse de kan forvente å møte dersom de kontakter politiet. Det er også varierende hvorvidt virksomhetene faktisks har tillit til at de vil få hjelp og om det er noe poeng i det hele tatt å levere anmeldelser og dele informasjon om datakriminalitet. Flere av informantene forteller at virksomhetene de jobber for har opplevd at når de kontakter politiet for å anmelde, til og med i store saker, ender det kanskje bare med henleggelser. Informantene tenker likevel at anmeldelsene og informasjonen kan bidra til at politiet får etablert et kunnskapsgrunnlag og at det kan bidra til statistikken når det kommer til datakriminalitet.

Informanter fra begge utvalgene påpeker at dersom ikke politiet evner å forebygge og håndtere datakriminalitet på en tilstrekkelig måte, vil dette kunne føre til at virksomheter og folk ellers mister tillit til politiet når det kommer til datakriminalitet. Sondre fra et privat sikkerhetsselskap fortalte hvordan håndteringen av vinningskriminalitet har kostet politiet tillit, og trekker direkte paralleller til håndteringen av datakriminalitet.

Når det kommer til kapasitet og kompetanse i forbindelse med datakriminalitet er det i dag store forskjeller innad i politiet. Flere av informantene i utvalg 2 forteller at politiet har utfordringer når det kommer til kapasitet og kompetanse, men at dette stiller seg forskjellig fra politidistrikt til politidistrikt, og hos Kripos som særorgan.

> Politiet har bygget et ganske robust kompetansesenter på Kripos, det som skalles NC3. Men det politiet som virksomhetene møter ute, det er de lokale politidistriktene, og der har vi en lang vei å gå. Jeg har vært borti virksomheter som har kontaktet lokalt politi for å anmelde også blir de sendt hjem igjen. Dette er jo noe vi må ta innover oss når vi driver og oppmuntrer virksomhetene til å anmelde, så er det jo gjerne lokalt politi som de møter, og da er det ikke sikkert de vil bli ivaretatt på en god måte når det kommer til datakriminalitet altså (Ruben, Politi- og lensmannsetaten).

Thomas, fra politi- og lensmannsetaten, forteller at det er få distrikter som er kapable til å etterforske datakriminalitetssaker alene. I tillegg er ofte datakriminalitetssakene store, alvorlige, komplekse og bærer preg av å være organiserte, noe som gjør at de ofte oppfyller kriteriene for å bli håndtert av Kripos. Han peker også på at datakriminalitetssaker krever mye kapasitet å etterforske, noe ikke distriktene alltid klarer å møte. Flere av informantene som er tilknyttet politi- og lensmannsetaten forteller hvordan ansvaret for forebygging og etterforskning i politidistriktene ofte blir pulverisert gjennom at polititjenestepersonene som får ansvar for datakriminalitet også gjerne har mange andre oppgaver og ansvarsområder.

> I distriktene handler det om kunnskap, kompetanse, ressurser og kapasitet. Politiet er på riktig vei, men distriktene må også med. Vi må ha formaliserte stillinger for datakriminalitet og egne miljøer for det. Avdelingene for digitalt politiarbeid (DPA) er flinke, men det er gjerne når det kommer til elektroniske spor osv. De har ikke noe spesielt «datakrim-fokus». Det er typisk at de personene i distriktene som jobber med elektroniske spor i andre typer saker også får ansvaret for etterforskning av datakriminalitet eller at dette havner hos de som jobber med økonomisk kriminalitet (Thomas, Politi- og lensmannsetaten).

Begge utvalgene påpeker at politiets kapasitet til å ta imot anmeldelser og etterforske datakriminalitet er for dårlig. Selv om NC3 er et stort steg i riktig retning er det stor skepsis til hvorvidt politiet evner å ta imot informasjon og anmeldelser på en god nok måte.

> Jeg tror det vil være dramatisk for politiet dersom virksomhetene i større grad velger å levere inn anmeldelser av datakriminalitet. Politiets kapasitet ville blitt utfordret. Samtidig tror jeg det vil være et viktig politisk signal for å få tilført flere ressurser. Hele politi-Norge må styrkes. Denne kriminaliteten er her nå. Hvis vi hele tiden skal være bakpå så går ikke dette. Vi ser jo nå under Covid-pandemien hva helsevesenet i Norge egentlig er, og hadde alt av virksomheter begynt å anmelde datakriminalitet så hadde vi også fått se hva politiet er (Patrick, Privat sikkerhetsselskap).

Blant informantene i utvalg 1 er det en tydelig usikkerhet rundt hva virksomhetene skal anmelde og ikke, og hvilken informasjon som egentlig er av interesse for politiet. I forlengelsen av dette er det også flere av informantene som gir uttrykk for frustrasjon ved at det ikke finnes enklere løsninger for å kunne anmelde og dele informasjon om datakriminalitet med politiet. Flere informanter i utvalg 2 påpeker at politiet må gjøre det enklere for virksomhetene å kunne levere inn anmeldelser og dele informasjon og mange nevner politiets nye tips-funksjon. Bård, fra politi- og lensmannsetaten, forteller at det ikke har vært noen tips-funksjon for datakriminalitet, men det har vært tips for mange andre fagområder. Dette har vært politisk styrt og bestemt, og i starten av 2021 ble tips-funksjonen for datakriminalitet endelig lansert politiets hjemmeside. Årsaken til det er at man må ha et system i bakkant som skal ta imot og håndtere det som kommer inn, noe politiet ikke har hatt.

I utvalg 1 trekker flere av informantene frem de har hatt negative møter med politiet, noe de opplever at bunner i en usikkerhet og kompetansenivå hos politifolk når det kommer til datakriminalitet. Manglende kompetanse og kunnskap på området har gjort at informantene eller kollegaer av dem i virksomhetene har hatt dårlige opplevelser i forbindelse med anmeldelser eller når de har forsøkt å rådføre seg om hva de skal gjøre i en situasjon i forbindelse med datakriminalitet.

> Det blir lite profesjonelt. Jeg har alltid tenkt at når du kommer til politiet så skal liksom det representere åpenhet, imøtekommenhet, kunnskap og trygghet. Politiet skal være en trygg havn og kommer du dit skal du få hjelp, råd og veiledning støtte osv., men når du kommer og får den opplevelsen av at politiet ikke helt ønsker å ta det imot, de prøver kanskje å skyve litt på det, «nei det skal kanskje til Økokrim, nei det tror jeg

> kanskje skal til NC3» osv., og denne opplevelsen vet jeg det er mange som har hatt! (Andreas, Teknologi og innovasjon).

Oppsummering politiets kompetanse, kapasitet og tillitsskapende arbeid

Begge utvalgene påpeker manglende kompetanse og kapasitet i politiet når det kommer til forebygging og håndtering av datakriminalitet. Politiets manglende evne til å ta imot anmeldelser og informasjon om datakriminalitet gjør det vanskelig for virksomhetene å både anmelde og bidra til politiets kunnskapsgrunnlag. I tillegg kan den manglende kompetansen og kapasiteten påvirke virksomhetenes tillit til politiets evne til å håndtere denne formen for kriminalitet, noe som igjen påvirker samarbeidet. Politiet har også kommet sent på banen når det kommer til denne problematikken, noe som kan ha ført til at andre, både offentlige og private aktører, har tatt et rom som politiet burde ha fylt. Likevel nevner informanter fra begge utvalgene at opprettelsen av NC3 i Kripos er et stort steg i riktig retning, men at også politidistriktene og kompetansen på datakriminalitet i hele politi-Norge må styrkes.

4.1.2 Politiets forebyggende strategi

Informantene som er knyttet til politi- og lensmannsetaten forteller om forebygging som politiets hovedstrategi, også i forbindelse med datakriminalitet. Bård, fra politi- og lensmannsetaten, forklarer at man i politiet har skjønt at det å «etterforske seg ut av» problemene knyttet til datakriminalitet er umulig og at det heller handler om å bidra til at publikum og virksomhetene settes i stand til å beskytte seg selv. Politiet er avhengig av å få informasjon om datakriminalitet fra virksomhetene for å etablere et kunnskapsgrunnlag å basere det forebyggende arbeidet på. Politiet vil også kunne få informasjon gjennom internasjonalt politisamarbeid, fra samarbeid med andre offentlige og private aktører som NSM og Mnemonic og fra publikum. Likevel er det viktig at politiet vet hva virksomhetene utsettes for både når det kommer til mindre alvorlig og alvorlig datakriminalitet. Flere av informantene fra politi- og lensmannsetaten forteller at informasjonen fra virksomhetene ikke nødvendigvis må komme i form av en anmeldelse. Samtidig må politiets kapasitet og satsning på datakriminalitet stå i stil med omfanget av det virksomhetene blir utsatt for.

> Det vi først og fremst mangler er ikke anmeldelser eller saker, men å vite hva som skjer. Men så er det også en balansegang. Vi kan jo fort se på et bilde hvor det er så mye datakriminalitet av vi kan bli litt tiltaksløse, også blir det kanskje bare til å se gjennom det vi har hver fullmåne, men hvis vi virkelig får opp fokuset og satsningen og synliggjør dette så kanskje vi etter hvert får ressursene til å ta tak i det. Hvis vi bare

> lar dette vokse og vokse og vokse så vil det bli et enormt samfunnsproblem, noe det egentlig allerede er (Thomas, Politi- og lensmannsetaten).

Flere av intervjuobjektene i utvalg 2 forklarer også at politiet trenger spesifikk informasjon fra dataangrepene for å kunne bruke dette videre, noe som også vil kreve at virksomhetene har kompetansen til å hente ut denne informasjonen eller får hjelp til det av en tredjepart. Dette er for eksempel informasjon om de kriminelle aktørenes fremgangsmåte og hva slags programvare som har blitt benyttet.

> Vi trenger jo mest mulig informasjon, men særlig logger som viser hva det er som har skjedd. Dersom det er løsepengevirus så er løsepengebrevene, kopi av infiserte filer, viktig slik at vi kan identifisere varianten og tidspunkter. Dersom offeret klarer å si noe om rekognoseringen, altså hvor lang tid angriperen var inne i systemet deres før de iverksatte angrepet, er det også viktig. For det vil jo til neste gang gi informasjon slik at det er lettere å etterforske, men også for å identifisere de sårbare punktene hos virksomheten som for eksempel tofaktorautentisering. Det er viktig for oss å avdekke dette for å gi virksomhetene god anbefaling og rådgivning i det forebyggende sporet (Thomas, Politi- og lensmannsetaten).

Informantene som er knyttet til politi- og lensmannsetaten forteller om at politiet har gjort fremskritt den siste tiden når det kommer til å benytte informasjonen som kommer frem gjennom informasjonsdeling fra virksomhetene til forebygging og avverging av datakriminalitet. I denne forbindelse trekkes det også frem at tidlig deling av informasjon og involvering av politiet er viktig i det forebyggende arbeidet.

> Forebygging og avverging hører jo tett sammen. Forebygging omhandler alle tiltakene man kan iverksette for å sikre seg selv i tillegg til å drive med bevisstgjøring hos folk. Også handler det om å få oppdatert informasjon om operativsystemer og sårbarheter. Så er det det avvergende som skjer når de er utsatt for angrep eller nesten er utsatt for angrep. Vi har flere eksempler på at informasjon som har kommet frem gjennom etterforskning forteller oss at flere norske firmaer har blitt utsatt for inntrengning, men vi har ikke hørt noe mer om det, så kanskje har de valgt å ikke si noe eller så vet de kanskje ikke om det. Da kan vi informere dem om dette slik at de kan fatte tiltak, og kanskje får vi det til før det har gått virkelig galt. Dette kaller vi varslingsaksjoner. Dette er kanskje ett av de viktigste tiltakene vi gjør (Bård, Politi- og lensmannsetaten).

Virksomhetenes forståelse av hva som er datakriminalitet og hvordan virksomhetene forholder seg til mindre alvorlig datakriminalitet og alvorlig datakriminalitet varierer. Dette spiller igjen inn på hva virksomhetene anmelder og når de tenker at det er viktig å kontakte politiet og ikke. Flere av informantene i utvalg 1 ga uttrykk for at de ikke vet hvordan politiet jobber med datakriminalitet eller hva politiet kan bidra med i denne forbindelse. De har fått med seg debatten rundt åpenhet og de fleste forklarer at de veldig gjerne vil dele informasjon med politiet når det kommer til datakriminalitet, enten dette er mindre alvorlige hendelser i det daglige som phising e-mail, forsøk på for eksempel direktørsvindel eller større dataangrep. For mange av virksomhetene handler dette om at de føler på et samfunnsansvar og de ønsker å hjelpe politiet i arbeidet med datakriminalitet. De ønsker også at de anmeldelsene de leverer og den informasjonen de deler skal bli en del av politiets statistikk slik at politiet kanskje kan få mer ressurser og at det vil synes i et større bilde. Flere av informantene påpeker også at de ikke nødvendigvis forventer at de skal få hjelp av politiet eller at det vil skje noe dersom de deler informasjonen, men de vet at det kanskje kan komme andre til gode gjennom det forebyggende arbeidet.

> På generell basis ønsker vi å dele så åpent som mulig, basert på en filosofi om at det kan komme andre til gode enten i Norge eller andre steder i verden (Karl, Transport).

Flere av informantene i utvalg 1 forklarer også at de har innsett at det ikke nytter å stå alene i møtet med datakriminalitet. Dette er også en av grunnene til at de ønsker å dele informasjon med politiet. Det er også mange av virksomhetene som er en del av større nettverk innad i bransjene hvor informasjonen deles på tvers. Pål fra Industri påpeker også at politiet ikke har vært en naturlig mottaker av informasjonen fra virksomheten hans og nettverket virksomheten er en del av grunnet politiets mottakerapparat, kapasitet og kompetanse på området.

> Informasjonsdeling er viktig når det kommer til håndteringen av datakriminalitet. Vi har etter hvert fått etablert gode nettverk mellom forskjellige aktører i privat næringsliv. Noe går via tjenesteleverandører, enten IT-tjenesteleverandører som f.eks. Sopra Steria eller Microsoft som har tatt store grep på sitt security økosystem og er flinke til å dele informasjon. Så i de store norske og internasjonale virksomhetene har det kommet på plass mye analysekapasitet når det kommer til vurderingen av trusler. Analytikerne både henter inn, prosesserer og bearbeider og gjør trusselvurderingene relevante for det gjeldende selskapet. Vi har lav terskel for å dele det på tvers. Vi deler ganske åpent, løpende og jevnlig spesielt hvis det er noe som haster. Det føles ikke

> like naturlig å dele dette med politiet, og noe av grunnen til det er at politiet ikke har hatt noen mottakersentral før man fikk NC3 (Pål, Industri).

Selv om hovedstrategien er forebygging påpeker Thomas at politiet også må få til noe mer. Politiet må også etterforske og ta tak i saker slik at denne formen for kriminalitet får konsekvenser for de kriminelle aktørene. Dette er viktig i det allmennpreventive og det individualpreventive arbeidet. I denne forbindelsen trekkes aksjonen som politiet hadde i Ukraina frem. Det viser at det nytter å dele informasjon med politiet og at politiet faktisk kan klare å straffeforfølge gjerningspersonene. Også informanter fra utvalg 1 trekker frem aksjonen i Ukraina som viktig. Dette skaper motivasjon for virksomhetene til å anmelde og dele informasjon med politiet. Selv om politiet er langt fra å få til dette i alle situasjoner viser det hvertfall at man er på vei i riktig retning.

En viktig del av politiets forebyggende strategi når det kommer til datakriminalitet er å få i gang en «dugnad», altså å etablere holdninger og et tankesett hos virksomhetene om hva hensikten er med å dele informasjon om datakriminalitet med politiet. Samtidig trekkes det frem av flere av informantene med tilknytning til politi- og lensmannsetaten at det er utfordrende å motivere virksomhetene til å anmelde og dele informasjon når det er begrenset hva politiet kan gjøre med situasjonen de står i og det er usikkerhet rundt om politiet klarer å gi noe i retur.

> Neste gang kan det være noen andre som blir rammet og gangen etter der er det kanskje den samme virksomheten som blir rammet igjen. Vi ser det at når vi forfølger sporene eller den digitale infrastrukturen og havner på disse kommando-kontroll-serverne som gjerningspersonene bruker for å begå kriminaliteten, så ligger det ofte ferdig konfigurerte sluttmål inne på den serveren. Og det er ofte sluttmål som har blitt kompromittert, men ikke kryptert, så du har et handlingsvindu og et tidsvindu hvor vi kan varsle om et mulig kommende angrep i andre virksomheter. Da kan vi si at dere har noen på innsiden av systemene deres, men dere er ikke kryptert enda. Så hvis dere agerer nå så kan dere rekke å beskytte dere. Og når vi går gjennom de serverne og finner virksomheter som har blitt kompromittert og kryptert, men som ikke har meldt dette til oss. Vi kan sette opp en tidslinje, og hvis da den virksomheten hadde sagt ifra, så kunne vi kanskje ha advart den og den og den virksomheten unngått å bli rammet. Vi hadde kommet tidligere til den serveren og vi hadde blitt satt i stand til å advare andre. Og her kommer dette med dugnad inn (Ruben, Politi- og lensmannsetaten).

I begge utvalgene trekkes politiets satsing på næringslivskontakter frem som et lyspunkt i politiets arbeid med datakriminalitet. Utvalg 1 mener at næringslivskontaktene er et fornuftig og effektivt kontaktpunkt mellom politiet og virksomhetene, og det gjør det enklere for virksomhetene å kommunisere og rådføre seg med politiet. Flere trekker også frem at det senker terskelen for å kontakte politiet fordi man har «et kjent fjes», altså en person man kanskje kjenner i den andre enden. Litt av grunnen til at dette kan senke terskelen går tilbake til dette med politiets kompetanse. Informantene i utvalg 1 synes det hjelper å vite at de kommer til en faglig kompetent person som har de riktige kontaktene innad i politiet, heller enn å skulle ringe inn til politiet eller møte opp på et publikumsmottak hvor de ikke nødvendigvis vet om de treffer på en kompetent polititjenesteperson når det kommer til å snakke om datakriminalitet. Likevel etterlyses det flere næringslivskontakter da etterspørselen er stor. I utvalg 2 trekker også flere av informantene frem viktigheten av næringslivskontaktene. Det kommer også frem at en sentral utvikling i arbeidet med næringslivskontaktene er å fylle på den digitale kompetansen og at det bør være næringslivskontakter i alle politidistrikt.

Oppsummering politiets forebyggende strategi

Selv om politiet skal etterforske og straffeforfølge datakriminalitet, er det forebygging som er politiets hovedstrategi i møtet med datakriminaliteten. Å «etterforske seg ut av» dette er ikke en gjennomførbar løsning, det handler heller om å sette virksomhetene i stand til å beskytte seg selv. For at politiet skal lykkes i det forebyggende arbeidet er politiet avhengig av å få informasjon fra forskjellige aktører, deriblant virksomhetene, for å danne et kunnskapsgrunnlag de kan basere den forebyggende virksomheten på. Politiet er opptatt av at vikromshetene skal se på arbeidet med datakriminaliteten som en «dugnad». Det hele må settes i et større perspektiv hvor virksomhetene anmelder og deler informasjon om hendelser til tross for at politiet kanskje ikke vil kunne straffeforfølge eller håndtere den enkelte hendelsen, men at informasjonen vil kunne brukes i et forebyggende og avvergende spor opp mot andre virksomheter. I neste runde er det kanskje virksomheten som ga informasjon som vil kunne oppleve å få noe tilbake fra politiet gjennom at noen andre har delt. Informantene knyttet til politi- og lensmannsetaten trekker frem at det er utfordrende å motivere virksomhetene til informasjonsdeling når det er begrenset hva politiet kan bidra med i retur.

Utvalg 1 gir uttrykk for at de ønsker å hjelpe politiet i dette arbeidet og at de opplever et samfunnsansvar. Samtidig er det flere i utvalg 1som gir uttrykk for at de ikke vet hvordan

politiet jobber med datakriminalitet og hvordan politiet kan nyttiggjøre seg av informasjonen. De ønsker likevel å bidra til kriminalitetsbekjempelse og politiets statistikk slik at politiet kan synliggjøre behovet for flere ressurser. I tillegg påpeker mange av informantene i utvalg 1 at virksomhetene forstår at det ikke nytter å stå alene i problematikken med datakriminalitet. Derfor vil de gjerne at politiet skal få denne informasjonen. Mange av virksomhetene har organisert seg i nettverk innad i bransjene for å dele informasjon. Denne informasjonen vil de også gjerne dele med politiet, men politiets kompetanse og kapasitet har gjort det vanskelig da politiet ikke har hatt et mottaksapparat.

Det er tydelig at det jobbes mot god informasjonsdeling i «begge leire», men at det fremdeles er utfordringer når det kommer til politiets kapasitet og kompetanse. Politiets arbeid med næringslivskontakter trekkes frem av begge utvalg som en positiv fremgang i politiets arbeid med forebygging.

4.1.3 Politiets kommunikasjon

I begge utvalgene påpekes det at det ikke er nok klarhet fra politiets side om hva slags informasjon politiet faktisk ønsker at virksomhetene skal dele, hva politiet trenger, hva som skal anmeldes og hvor informasjonen skal rutes. Et stort dataangrep vil kanskje skille seg ut fordi virksomhetene trenger hjelp, og det er en del av noe større som politiet gjerne vil være delaktige i å jobbe med. Sondre i et privat sikkerhetsselskap forteller at de fleste uønskede digitale hendelsene som virksomhetene opplever er datakriminalitet, og i teorien skal da enhver phishing-epost og hvert eneste forsøk på å bryte gjennom brannmurer osv. anmeldes. Han påpeker at det ikke har blitt sendt noen tydelige signaler fra politiet om hvor terskelen går for hva virksomhetene skal anmelde og ikke og hvordan de skal forholde seg til disse hendelsene. Harald, som jobber i et offentlig myndighetsorgan, mener at politiet med fordel kan være mer aktive ute i det offentlige for å tydeliggjøre sin rolle og formidle terskelverdiene for når politiet skal kontaktes i forbindelse med datakriminalitet. Dette handler også om en tydeliggjøring av at datakriminalitet må ses på som kriminalitet på lik linje med «vanlig» kriminalitet.

> Politiet bør fortelle litt mer om hvordan de jobber og går frem i sånne saker slik at det kan tjene som en forventningsavklaring og tydeliggjøre hva som kreves. Det kan også bidra til å gjøre det mindre «skummelt» å anmelde forholdet. Også må politiet være åpne om at dette er en samfunnsviktig utfordring, og bevisstgjøre folk. Det er lurt å formidle en forventningsavklaring til hva politiet gjør i sånne saker. Det må komme

> frem hvilken rolle politiet har, det må skapes en bevissthet i samfunnet rundt at dette er kriminalitet på lik linje med mye annet og at man har en forventningsavklaring til hva som skjer dersom man kontakter politiet (Harald, Offentlig myndighetsorgan).

Flere informanter fra utvalg 1 forteller om usikkerhet knyttet til hva politiet kan hjelpe virksomhetene med når det kommer til datakriminalitet og når politiet egentlig ønsker at virksomhetene skal dele informasjon om datakriminalitet og anmelde hendelser. Flere påpeker at de ikke ønsker å kontakte politiet med anmeldelser og informasjon bare for å gjøre det, noe som har bakgrunn i en oppfattelse av at politiet allerede har knapt med ressurser og kapasitet. Pål fra Industri forteller om en opplevelse han ikke er alene om å ha, nemlig at politiet sier «anmeld all datakriminalitet». Pål sin opplevelse var fra en sikkerhetskonferanse som Næringslivets sikkerhetsråd holdt hvor en representant fra Politidirektoratet stilte på scenen og anbefalte virksomhetene å anmelde all datakriminalitet, noe som skjer «år etter år». Dette bidrar til å bygge opp forventninger hos virksomhetene og kan virke forvirrende når politiet ikke evner å ta imot anmeldelsene eller at det ikke gjøres noe når virksomhetene anmelder.

> Se på antallet angrep vi har da, eller antall forsøk. Også er det jo dette med å definere hva som er forsøkets nedre grense i datakriminalitet. Vi har fått en skadevare tilsendt, men vi har beskyttende mekanismer. Er det et straffbart forhold eller ikke? Skal vi anmelde eller ikke? Hvis jeg hadde samlet opp alt det jeg definerer som straffbare forhold i min virksomhet så måtte vi ha hatt en liten hær på politistasjonen som bare satt og tok imot anmeldelser (Pål, Industri).

Flere informanter i utvalg 2 forteller at det verken er ønskelig eller hensiktsmessig at virksomhetene skal «anmelde alt alltid» når det kommer til datakriminalitet, men de vet at dette ofte blir kommunisert ut. Ruben fra politi- og lensmannsetaten forteller om en kollega som i en samtale med en virksomhet hadde anbefalt virksomheten nettopp å anmelde alt, hvor virksomheten hadde svart med at de hadde 35.000 anmeldelser de kunne levere fra det forrige året, politiet måtte bare si hvor de ville ha det. Informantene med tilknytning til politi- og lensmannsetaten forteller at politiet har måttet legge seg på en linje hvor man ønsker at virksomhetene skal anmelde, samtidig som det er viktig å informere om at det ikke er sikkert saken blir fulgt opp. Samtidig vil informasjonen bli tatt tal i og koordinert internasjonalt. Dette kan bidra til å berike et bilde og kanskje er det akkurat de opplysningene virksomheten kommer med som kan hjelpe en etterforsker i et annet land med å løse en sak. Dette er i tråd med tanken om en «dugnad». Datakriminalitet er et internasjonalt problem som gjør at politiet må samarbeide og dele informasjon på tvers av landegrenser. Dersom en virksomhet ikke

ønsker å anmelde så kan politiet likevel ta imot informasjonen uten forpliktelsene som følger med en anmeldelse. Informantene forteller videre at dersom politiet oppfordrer virksomhetene til å anmelde alt alltid vil dette kunne bygge opp forventninger hos fornærmede som vil kunne bli knust. En annen utfordring som raskt melder seg i denne forbindelse er at politiet heller ikke har etablert et kodeverk som gjør at politiet kan få tilstrekkelig oversikt over datakriminaliteten som anmeldes. Dette utfordrer politiets evne til å målrette den forebyggende innsatsen. Dette knyttes også til politiets kapasitet og kompetanse når det kommer til datakriminalitet.

> Den nye straffeloven skulle være teknologinøytral, så et løsepengevirus er i teorien fire lovbrudd; datainnbrudd, tyveri fordi det eksfiltreres informasjon, skadeverk i form av kryptering og utpressing i form av løsepengekravet. Og hva dette blir kodet på rundt omkring i forskjellige politidistrikt, det har jeg sett mye rart på altså. Og dette er et fagfelt som politifolk kvier seg litt for å ta. Så det der med å ha et argument om at vi må ha opp statistikken det fungerer også dårlig for vi har jo ikke et kodeverk som egner seg å bruke (Ruben, Politi- og lensmannsetaten).

I begge utvalgene kommer det tydelig frem at informantene ikke synes politiet er synlig nok i mediebildet og samfunnsdebatten når det kommer til datakriminalitet, og at politiet bør ta mer eierskap til sitt mandat og synliggjøre dette. Også her nevnes det av flere at dette rommet fort blir tatt av andre, både private og offentlige aktører. Det er tydelig at informantene i utvalg 1 ønsker at politiet skal være mer tydelig og synlig rundt sin rolle og sitt ansvar når det kommer til datakriminalitet. Flere av informantene i dette utvalget nevner at de ofte ser NSM og andre aktører i mediebildet, noe som også gjør at man ikke like enkelt assosierer politiet med datakriminalitet. Informanter fra utvalg 2 mener at politiet bør fokusere på å bygge tillit med publikum og virksomhetene gjennom å være mer synlige utad og kommunisere hva politiet kan gjøre både i det forebyggende og avvergende sporet. At politiet ikke synes så godt i mediebildet når det kommer til datakriminalitet trekkes også frem som noe som kan bidra til at virksomhetene ikke i like stor grad assosierer uønskede digitale hendelser eller datakriminalitet med politiet. Politiet bør vise at de både driver med mer «tradisjonell» kriminalitet, men også datakriminalitet. Informantene med tilknytning til politi- og lensmannsetaten forteller at politiets kapasitet og kompetanse kan ha bidratt til at politiet har holdt seg litt unna mediebildet og samfunnsdebatten.

> Jeg synes vi burde vært veldig mye mer frempå. NSM og Forsvaret for eksempel er jo veldig gode på å plassere seg selv i landskapet og tar naturlig plass. Samtidig er jo det

> som skjer av cyberkriminalitet, eller datakriminalitet, politiets oppdrag. Er det kriminalitet så er det politiet. Så vi må være tydeligere på å kommunisere at det er ikke alltid sikkert det er en statlig aktør, og er det datakriminalitet så er det politiet som skal kontaktes. Vi er veldig bevisste det at vi må være flinkere her. Pushe oss selv litt frem, i tillegg å være på tilbudssiden når vi blir invitert til noe. Samtidig er det jo ikke riktig at politiet gjør seg høye og mørke hvis vi ikke har noe å vise frem. Det er jo først etter etableringen av NC3 at vi har kunnet slå på stortromma og vise til noe, at vi har ressurser, kapasitet, kompetanse, og evnen til å håndtere denne typen saker mye mer enn hva vi hadde før. Dette blir det kanskje enda mer av i fremtiden med en større etablering av næringslivskontakter også. Når politiet har store aksjoner så bidrar jo dette til en bevissthet blant folk om politiet også jobber med datakriminalitet (Bård, Politi- og lensmannsetaten).

Informanter fra begge utvalgene trekker frem viktigheten av «solskinnshistorier», altså å vise frem den jobben politiet gjør når man har lykkes i noe i forbindelse med datakriminalitet. Aksjonene som ble gjennomført i Ukraina trekkes frem av flere som en historie som bidrar til å synliggjøre jobben politiet gjør, noe som puster liv i tillit og håp om at politiet skal få på plass kapasitet og kompetanse for å virkelig delta i kampen mot datakriminaliteten.

> Jeg opplever jo etter det jeg leser i mediene og det jeg hører er at NC3 sin tilnærming til datakriminalitet nå er veldig bra. Spesielt at man faktisk fant dem som stod bak dataangrepet mot Hydro. Meget viktig. At det etterforskes og at det faktisk bærer frukter. Så det ikke bare er et «svart hull» som man informasjon i og at attribusjon kan man bare glemme og vi klarer hvertfall ikke å pågripe dem! (Ole Gunnar, Finans).

I utvalg 1 er det flere av informantene som nevner at de ønsker at politiet skal invitere til seminarer og dele av sin kunnskap, erfaringer og informasjon om datakriminalitet. Det er ikke fordi slike seminarer er mangelvare, tvert om, men mange av virksomhetene ønsker at informasjonen skal komme fra politiet og ikke aktører som kanskje presenterer et budskap med en agenda sånn som de opplever at en del av de store private sikkerhetsselskapene gjør. Det betyr ikke at informasjonen de private selskapene presenterer er feil, men politiet kunne i større grad bidratt til å skape en nøytral arena for informasjonsdeling. Virksomhetene ønsker informasjon som kan hjelpe dem i beredskapsarbeidet og med å beskytte seg mot datakriminalitet og påpeker at dersom informasjonen kommer fra politiet har det stor verdi og kraft.

Oppsummering politiets kommunikasjon utad

I begge utvalg mener informantene at det ikke nødvendigvis er hensiktsmessig virksomhetene skal anmelde all datakriminalitet. Det har ikke politiet per dags dato kapasitet eller kompetanse til å håndtere, og det vil heller ikke bidra til et statistisk grunnlag på grunn av et manglende kodeverk og system hos politiet. Det jobbes med å få på plass et system for dette i politiet, men det tar tid og informantene i utvalg 1 savner en uttalt forventningsavklaring fra politiet og informasjon om status i arbeidet og hva de skal forholde seg til når det kommer til anmeldelser og informasjonsdeling. Det er viktig at politiet ikke skaper usikkerhet og frustrasjon gjennom å kommunisere at all datakriminalitet skal anmeldes, når dette ikke er hensiktsmessig. Informanter med tilknytning til politi- og lensmannsetaten forteller om viktigheten av at politiet forklarer virksomhetene hva de kan forvente og hvorfor informasjonsdeling er viktig selv om det kanskje ikke hjelper virksomheten der og da. Politiet trenger informasjon fra virksomhetene om datakriminalitet, men dette trenger ikke å skje gjennom anmeldelser. Informasjonen om datakriminalitet bidrar til at politiet kan etablere et kunnskapsgrunnlag og få et godt situasjons- og trusselbilde, noe som igjen vil kunne bidra til at politiet kan identifisere og formidle klare og målrettede tiltak gjennom det forebyggende sporet slik at virksomhetene kan beskytte seg.

Begge utvalgene mener at politiet med fordel kan ta mer eierskap til tematikken gjennom å være mer tydelig og synes i mediebildet og samfunnsdebatten. Dette vil kunne bidra til å gjøre politiets rolle i datakriminalitet bedre kjent, noe som igjen kan gjøre at politiet seiler opp som en aktuell aktør for virksomhetene å samarbeide med. Selv om flere av informantene som er tilknyttet politi- og lensmannsetaten forteller at politiet er klar over dette, forteller de også at dette kan forklares på samme måte som at politiet har kommet litt sent på banen når det kommer til datakriminalitet. Solskinnshistorier blir trukket frem som viktig både i utvalg 1 og utvalg 2. Slike suksesshistorier som viser hvordan politiet jobber og at det også kan få positive utfall er med på å motivere virksomhetene til å samarbeide og dele informasjon med politiet, samtidig som politiet får vist sin rolle og sin plass i tematikken.

4.1.4 Politiet og de andre aktørene

Informanter fra begge utvalgene påpeker at det er overlappende mandater og oppgaver mellom politiet og andre offentlige aktører. Spesielt trekkes NSM og NCSC frem. Flere påpeker at mye av informasjonen som burde deles med politiet fort blir gitt til NSM og NCSC fordi de har hatt et mottaksapparat lenger enn det politiet hat hatt gjennom Kripos og NC3, i

tillegg til at NSM har vært flinke til å kommunisere godt ut til virksomhetene og etablere et velfungerende samarbeid med næringslivet og det offentlige når det kommer til forebygging og håndtering av digitale trusler. I utvalg 2 er det flere som beskriver et godt samarbeid mellom NSM og politiet når det kommer til datakriminalitet, og at NSM har fått den posisjonen de har handler mye om at de har kommet tidligere på banen enn politiet og at de har gjort en svært god jobb med å gjøre seg tilgjengelige og relevante. Det er heller ikke sånn at informasjonen utelukkende skal til kun ett myndighetsorgan, ofte er det riktig at informasjonen har flere mottakere. Det må likevel koordineres på en god måte og det må kommuniseres til virksomhetene.

I utvalg 1 er det flere av informantene som påpeker at de ser på det som mer naturlig å kontakte NSM og NCSC når de opplever et dataangrep eller mindre alvorlige uønskede digitale hendelser fordi de ikke tenker at dette nødvendigvis er noe som skal til politiet. Andre påpeker at de er usikre på hvilke offentlige aktører som er riktige å kontakte i de forskjellige tilfellene og at de ikke helt forstår ansvars- og rollefordelingen mellom for eksempel NCSC og NC3. Mange er heller ikke så opptatte av akkurat hvilken informasjon som skal til hvilket offentlig myndighetsorgan, mest at informasjonen blir koordinert, at de får den hjelpen og de rådene de trenger og at de som jobber i myndighetsorganene har kontroll på hvordan informasjonen skal forvaltes.

I utvalg 2 påpeker Thomas, fra politi- og lensmannsetaten, at virksomhetene mest sannsynlig kontakter dem som de kan få noe igjen fra når de trenger det, og lenge har dette vært NSM gjennom den kapasiteten de har bygd gjennom NCSC. Videre sier han noe som også flere i utvalg 1 har nevnt, nemlig at datakriminalitet eller hendelser som faller innunder definisjonen av datakriminalitet og omfattes av straffeloven ofte blir omtalt som datasikkerhetshendelser, informasjonssikkerhetshendelser og lignende. Dette mener han at kan handle om vårt forhold til disse hendelsene og forståelsen vår for hva som er datakriminalitet og ikke. Det er akkurat som at man ikke tenker på det som like straffbart som annen kriminalitet, eller at det er så lite håndfast at det blir litt diffust å forholde seg til.

Harald, fra et offentlig myndighetsorgan, mener at politiet, NSM og andre offentlige organer som jobber med datakriminalitet og datasikkerhet må kommunisere godt seg imellom og dele informasjonen for at de offentlige instansene som arbeider med forebygging og håndtering av trusler fra cyberdomenet ikke skal snuble i beina på hverandre. Han mener videre at kommunikasjon og god koordinering er viktig slik at innsatsen fra det offentlige fremstår profesjonell og samlet ovenfor virksomhetene, men også for at de ikke skal måtte

forholde seg til for mange myndighetsaktører. Virksomhetene og samfunnet må også få en bedre forståelse for hvordan man skal se på hendelsene, og at dette er like mye kriminelle handlinger som om noen skulle ha brutt seg inn hjemme hos deg.

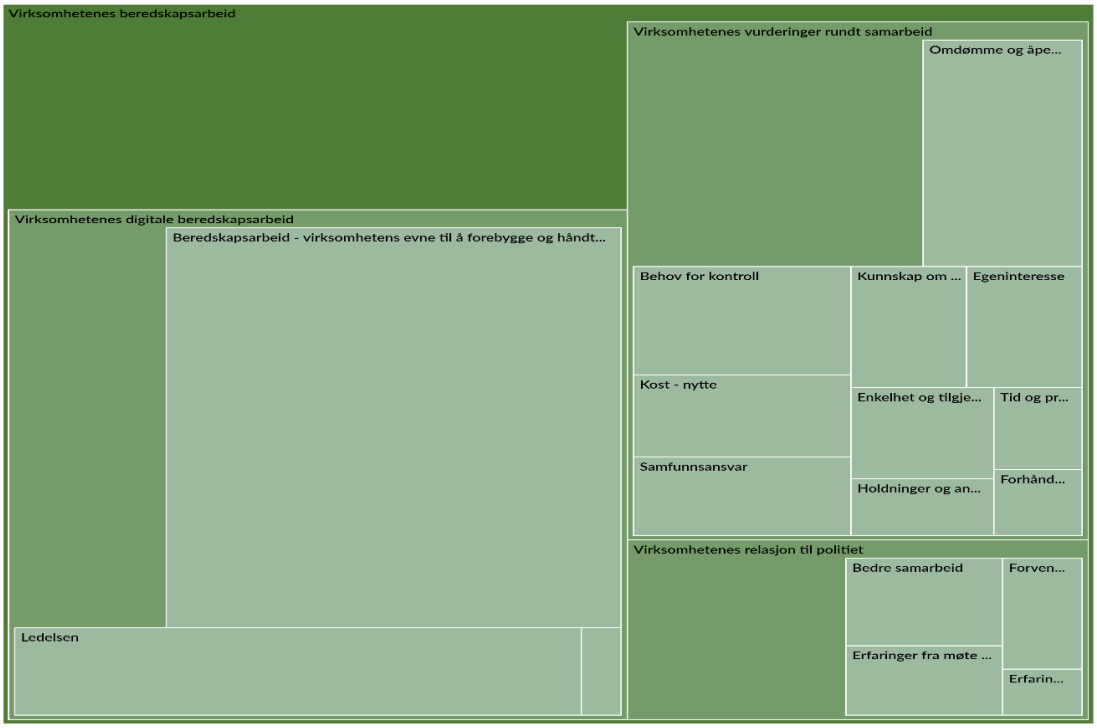
Ruben, fra politi- og lensmannsetaten, trekker også frem politiets avtaler med private aktører. En av de politiet har en slik avtale med er Mnemonic. Det er flere virksomheter som får bistand fra private aktører når de blir utsatt for datasikkerhetshendelser eller datakriminalitet. På den måten blir politiets kjennskap til og relasjon til disse aktørene viktig. Samarbeidsavtalene med de private aktørene er et forsøk på å få på plass et bedre samarbeid både på "åstedet", altså hos fornærmede som her gjerne er virksomhetene, men også når det kommer til deling av informasjon til bruk i det forebygging.

Oppsummering politiet og de andre aktørene

De overlappende mandatene og arbeidsoppgavene til de forskjellige myndighetsorganene gjør at det er vanskelig for virksomhetene å forstå hvem som er riktig å kontakte. I tillegg har for eksempel NSM vært på banen lengre enn politiet og de har vært flinke til å gjøre seg tilgjengelige og relevante. På denne måten er det flere av virksomhetene som heller tenker på NSM når det kommer til datakriminalitet enn på politiet. I utvalg 2 fremkommer det at det er et godt samarbeid mellom de offentlige myndighetsorganene når det kommer til datakriminalitet, noe som spesielt har utviklet seg etter etableringen av NC3. I tillegg jobber politiet med å få på plass samarbeidsavtaler med private aktører som Mnemonic, noe som vil bedre det forebyggende arbeidet og skape et godt grunnlag for informasjonstilgang. Det viktigste er at koordineringen og samarbeidet mellom de offentlige myndighetsorganene fungerer bra i arbeidet med datakriminaliteten. En hendelse kan treffe mandatet til flere enn politiet. Likevel ønsker informantene i utvalg 1 at det skal komme tydeligere frem hvilke roller de forskjellige har og hvordan de samarbeider, men aller viktigst er det at de får den hjelpen de trenger og blir satt i kontakt med de riktige aktørene uansett hvem de henvender seg til.

4.2 Virksomhetenes beredskapsarbeid

I dette underkapitlet presenteres hovedkategori 2 «Virksomhetenes beredskapsarbeid». Figur 4.7 viser en fremstilling av hovedkategorien med underkategorier.



Figur 4.7 Oversikt over hovedkategori 1 – Politiet og datakriminalitet fra NVivo

Jeg vil videre gå nærmere inn på hovedkategori 2 og de forskjellige underkategoriene i første linje og deres underkategorier i andre linje der det er hensiktsmessig. Virksomhetenes beredskapsarbeid ble et sentralt tema i alle intervjuene.

4.2.1 Viktigheten av gode forberedelser

Informanter fra begge utvalgene forteller om hvordan virksomhetenes beredskapsarbeid er sentralt i hvordan virksomhetene forholder seg til politiet når det kommer til datakriminalitet. Samtidig er det stor variasjon i hvordan virksomhetene forholder seg til arbeidet med beredskap. Det som blir trukket frem som den viktigste faktoren i dette er hvorvidt en virksomhet gjennom arbeidet med beredskap har tatt stilling til hvordan de skal forholde seg til politiet når det kommer til datakriminalitet. Dette kan både gjelde mindre alvorlig datakriminalitet i det daglige, eller hvordan virksomheten skal forholde seg til politiet dersom de blir utsatt for alvorlig datakriminalitet. Flere av informantene i begge utvalgene nevner begrepet «modenhet» i denne sammenheng, noe som de knytter til virksomhetens arbeid med beredskap, hvordan ledelsen forholder seg til utfordringene knyttet til temaet, hvordan virksomheten sikrer seg både når det kommer til menneskelige, organisatoriske og tekniske forhold, og hvordan de forstår og forholder seg til trusselen som datakriminalitet utgjør.

> Når det kommer til en virksomhets beslutning om å kontakte politiet eller ikke i forbindelse med datakriminalitet tror jeg overordnet at dette handler om modenhet.

> Hvis vi ser helt banalt på det; det skjer en hendelse. Skal vi virksomheten varsle politiet ja eller nei? Jeg tror at flere virksomheter rett og slett ikke tenker på det. De er så umodne at når de først står i situasjonen så har de bare ikke peiling på hvordan de skal agere, rett og slett. Da blir det kanskje heller til at de ringer en privat rådgiver eller konsulentbedrift og så kommer det noen for å gi dem råd. Også kan det jo hende at de blir gjort oppmerksomme på at de burde varsle politiet (Sondre, Privat sikkerhetsselskap).

De informantene i utvalg 1 som jobber for en virksomhet som har opplevd å bli utsatt for alvorlig datakriminalitet, i disse tilfellene dataangrep, forteller om en kaotisk og uoversiktlig initialfase preget av tidspress og usikkerhet. I denne fasen er det mange arbeidsoppgaver som skal dekkes og informantene forteller at virksomheten egentlig har mer en nok med å håndtere krisen internt. Vibeke fra Industri forteller at da hennes virksomhet opplevde dette for første gang hadde de ikke kunnskap om at politiet burde kontaktes, og det var heller ikke noe de hadde tatt høyde for i beredskapsplanene.

> Det vi gjorde veldig tidlig var at vi fikk kontakt med andre selskaper som hadde vært utsatt for det samme og søkte råd der. Og det var jo andre selskaper i andre land, og det var ingen av de som fremhevet kontakt med politiet. Så i løpet av den første dagen så var vi rett og slett ikke kommet dit at vi hadde bevissthet rundt at det å kontakte politiet var en klok ting å gjøre (Vibeke, Industri).

Flere av informantene i utvalg 2 legger stor vekt på at forberedelser er det aller viktigste for å få til et godt samarbeid mellom virksomhetene og politiet. I denne sammenheng blir det trukket frem at virksomhetene bør starte med en kartlegging gjennom for eksempel å bruke en modenhetsanalyse eller gjennom bruk av et standardisert rammeverk. Allerede gjennom dette arbeidet kan virksomhetene få mange «quick wins», altså gjøre enkle tiltak som vil heve sikkerhetsnivået betraktelig. En grunnleggende kartlegging vil kunne gi en oversikt over virksomhetens svakheter og danner et godt utgangspunkt for det videre beredskapsarbeidet. Dette vil gi oversikt over hva man trenger å beskytte, og ikke minst hva konsekvensene vil være dersom det går ordentlig galt. Informantene i utvalg 2 forteller at det er mange virksomheter som ikke tror at de er så aktuelle for ondsinnede aktører, men det vil alltid være noen som er interesserte i å utnytte sårbarhetene til virksomhetene. Noen av informantene med tilknytning til politi- og lensmannsetaten forteller at virksomhetene kan få rettet opp i mye, men man får ikke rettet opp i informasjon på avveie til fri benyttelse for kriminelle aktører. I den forbindelse fremhever de at det er viktig at virksomhetene gjennomfører en

konsekvensanalyse som gir virksomhetene anledning til å ta innover seg hva som skjer dersom det går skikkelig galt. Det handler om hvordan virksomhetene tolker og opplever trusselen fra datakriminelle og forstår hva de kan bli utsatt for.

Informantene i utvalg 1 som representerer virksomheter som har opplevd å bli utsatt for alvorlig datakriminalitet trekker frem hvordan fokuset på dette med å inkludere det digitale elementet i virksomhetens arbeid med beredskap fikk en større forankring i virksomheten etter at de ble utsatt for dataangrep. De forteller også hvordan de har fått en mer helhetlig tilnærming til sikkerhet hvor ikke digital sikkerhet lenger er noe som settes til IT-avdelingen og blir noe som ikke resten av virksomheten bryr seg om. Informanter fra utvalg 2 trekker frem at i tillegg til å jobbe med beredskap og etablere et godt beredskapsplanverk er det viktig at virksomhetene faktisk operasjonaliserer tiltakene kommer ut av beredskapsarbeidet og at dette er noe som varierer veldig hos virksomhetene. Dessverre er det flere virksomheter som nøyer seg med å bare gjennomføre analysene og skrive beredskapsplanene, men når det går galt viser det seg at planverket ikke fungerer i praksis eller at virksomheten ikke får utnyttet potensialet i planene fordi de ikke har testet det ut gjennom for eksempel trening og øving. Flere informanter i utvalg 2 forteller også at de har respekt for den komplekse situasjonen virksomhetene står i med å forholde seg til et digitalt trusselbilde i stadig endring. Informantene har opplevd å treffe på virksomheter som har blitt utsatt for alvorlig datakriminalitet, hvor de ikke er spesielt stolte når det avdekkes hvor lavt sikkerhetsnivå de har hatt. Informantene trekker frem at det i slike situasjoner er viktig å innta en mer støttende tilnærming. Det er viktig at virksomhetene har tillit til myndighetene og at myndighetene ivaretar ulike hensyn og interesser. Slik trusselbildet er i dag er det vanskelig for en virksomhet å sikre seg mot alt, og alle kan gjøre feil. Da er det viktig å dra lærdom av disse feilene.

Flere av informantene i utvalg 1 forteller at fokuset på digital sikkerhet økte betraktelig etter dataangrepet som rammet Hydro i 2019. Det er forskjellig hvordan virksomhetene jobber med dette. Flere av informantene nevner også at de fokuserer på sikkerhet i hele virksomheten og at sikkerhet handler om helhet. Ole Gunnar, som jobber i Finans, påpeker at sikkerhet i dag ikke bare handler om det fysiske eller digitale domenet, det er summen av alt. Den digitale sikkerheten har på denne måten blitt tatt med inn i virksomhetens beredskapsarbeid, og flere av informantene forteller også at de ikke bare fokuserer på de som jobber direkte med dette, men at det er viktig at alle blir med og at det etableres kollektiv digital sikkerhetskultur.

4.2.1.1 Trening og øving

Et annet moment som trekkes frem av informanter fra begge utvalgene er viktigheten med trening og øvelse som en del av beredskapsarbeidet. En av informantene i utvalg 1 fortalte hvordan dette var en suksessfaktor da virksomheten han jobber for utsatt for et dataangrep.

> Vi har organisert og tatt del i en rekke beredskapsøvelser knyttet til dataangrep. Da vi ble utsatt for dataangrep var det helt vesentlig for oss at vi faktisk hadde øvd på et lignende scenario. Vi har beredskapsplaner og krisehåndteringsplaner og kontinuitetsplaner, men når virkeligheten treffer så er det et lite stykke fra teori til praksis. Jeg føler meg ganske trygg på at viktigheten av trening og øvelse kommer til å bli løftet ganske høyt i evalueringen av hendelseshåndteringen. Det var tenkt gjennom scenarioer alt fra hva gjør vi med selve systemet, hvordan tar vi de ned, hva gjør vi for å få de opp til hvordan er kommunikasjonslinjene, hvordan snakker vi med kunder, leverandører, politiet og andre myndigheter? Det å ha øvd på dette opplevde vi som veldig viktig (Kåre, Matproduksjon).

I utvalg 1 er det flere av informantene som snakker om kostnaden av sikkerhet. Mange mener at dette er noe som skiller de store, mellomstore og små virksomhetene fordi sikkerhet ofte er dyrt, noe som kan by på utfordringer når ledelsen skal allokere midler og ressurser. I denne sammenheng er det også flere som nevner at det er umulig å sikre seg 100% og at datakriminaliteten ofte er så sofistikert og profesjonell nå at dersom de kriminelle ønsker å «komme seg inn» så får de til det, uavhengig av hvor god sikkerheten er. Dermed er det vanskelig å argumentere for at store deler av virksomhetens budsjett skal brukes på sikringstiltak. Flere av informantene påpeker at det i denne sammenheng er viktig at sikkerhetsarbeidet er forankret i ledelsen og at ledelsen har forståelse for hva som må til for å opprettholde god sikkerhet. Samtidig er det flere som påpeker at det å drive beredskapsarbeid og planlegge hvordan virksomheten skal organisere seg dersom man blir utsatt for alvorlig datakriminalitet er «gratis». Dette er noe virksomheten derimot må avse tid og kapasitet til. Av de virksomhetene som har gjennomført beredskapsarbeid med fokus på rutiner og organisering og sett nytten av det er det ingen tvil om at de er fornøyde med å ha lagt ned tid og kapasitet i dette arbeidet. Dette har blant annet bidratt til at de har gått opp kommunikasjonskanalene og rutinene med politiet og myndigheter og føler seg mindre usikre på hvordan de skal gå frem dersom en uønsket hendelse skulle inntreffe. Også informanter fra utvalg 2 forteller om tiltak virksomhetene kan gjøre som ikke koster penger. Ruben, fra politi- og lensmannsetaten, forteller at han har truffet flere virksomheter som har gjennomført

øvelser knyttet til datakriminalitet hvor virksomhetene har opplevd stor virkning av dette. Flere av informantene i utvalg 1 trekker politiets også frem politiets kompetanse når det kommer til å drive kriseledelse som noe som gjør et samarbeid med og en involvering av politiet attraktiv, nettopp fordi virksomhetene ikke har den samme kompetansen når det kommer til denne typen ledelse.

4.2.1.2 Kommunikasjonsstrategi

Intervjuobjekter fra begge utvalg fremhever kommunikasjonsstrategi som en viktig del av beredskapsarbeidet. Dette handler både om å klare å håndtere media midt i krisen, men også å ha kontroll på informasjonen som kommer ut for å ikke skape en større krise. Her vil et godt samarbeid med politiet være essensielt fordi politiet også vil kunne få stor medieoppmerksomhet rundt hendelsen. Her forteller flere av informantene i utvalg 1 at det vil være viktig for dem å få lov til å «styre narrativet», og at kommunikasjonen utad både fra virksomheten og politiet må samkjøres.

> Det som er interessant er jo at hvis du skal være god på å håndtere digitale trusler og sårbarheter og du faktisk blir utsatt for et angrep, så må du også være god på strategisk krisekommunikasjon. For det kan gjøre krisen større ved å håndtere den dårlig i media. Og når det kommer til det digitale domenet skal du være ganske kjapp på avtrekkeren for hvordan du håndterer det internt, ut i samfunnet, men også til kunder og leverandører. Hvis ikke dette er på stell så vil man mulig kunne gå på et omdømmetap eller lage krisen større. Vi kan kalle dette forberedelser. Du må ha lagt planer og du må ha trent på det (Patrick, Privat sikkerhetsselskap)

Når krisekommunikasjon nevnes i forbindelse med datakriminalitet, som for eksempel ved et dataangrep, handler det også om taktiske og strategiske valg når det kommer til hvilken informasjon man går ut med. Det er mye usikkerhet i starten av et dataangrep, i likhet med andre kriser. Her er det viktig å tenke gjennom hvordan man skal kommunisere og hva man skal kommunisere. Man må også ta høyde for at det sitter en ondsinnet aktør på den andre siden som også vil kunne få med seg informasjonen, og man vil nødig gi ut informasjon som denne aktøren kan nyttiggjøre seg av.

Kåre forteller at hans oppfattelse er at virksomheter ikke lenger synes det er så ille å være åpne om at de har blitt utsatt for et dataangrep, men at virksomhetene vil ha et stort behov for å styre hvilken informasjon som kommer ut med tanke på den komplekse målgruppen de skal forholde seg til. Han trekker frem viktigheten av et godt samarbeid med

politiet og andre myndighetsaktører når det kommer til kommunikasjonen utad. Forskjellige virksomheter vil ha forskjellige behov, men det er viktig at man har tenkt gjennom dette slik at virksomheten kan få til et godt samarbeid med politiet og politiets kommunikasjon utad om en hendelse.

4.2.1.3 Kunnskap og kompetanse

Når de to utvalgene forteller om viktigheten av kunnskap og kompetanse hos virksomhetene når det kommer til digital sikkerhet og datakriminalitet, ser de dette fra to perspektiver. Det ene er hvorvidt virksomheten evner å bygge opp en kompetanse på digital sikkerhet og datakriminalitet gjennom hele virksomheten, helt fra et teknisk ekspertnivå til brukerkunnskap hos de ansatte, noe som baserer seg på tanken om en sikkerhetskultur. Det er viktig at man har en kultur hvor alle i virksomheten, på ulike nivåer, har kunnskap om datasikkerhet. Det andre er hvorvidt virksomhetene har tilgang til kompetanse, da det er viktig at virksomheten får tak i mennesker med den riktige kompetansen for å opprettholde den digitale sikkerheten rent teknisk. I utvalg 1 forteller flere av virksomhetene om viktigheten av å være en del av et nettverk hvor man deler informasjon om datasikkerhetshendelser og datakriminalitet. Hensikten med og tanken bak disse nettverkene er på mange måter det samme som politiet ønsker å oppnå gjennom å drive informasjonsinnhenting og danne et kunnskapsgrunnlag. Informantene i utvalg 1 forteller også om at det er et ønske at politiet skal kunne dele informasjon med dem, noe som strekker seg ut over det de får gjennom nettverkene de er en del av. Dette vil kunne bidra til at virksomhetene øker sin kunnskap og kompetanse når det kommer til datakriminelle og et trusselbilde i stadig utvikling. De fleste av informantene i utvalg 1 har enten bygget kompetanse og et fagmiljø i sin egen virksomhet eller de har etablert gode avtaler med sikkerhetsselskaper som bistår dem i arbeidet med digital sikkerhet. I tillegg er de fleste opptatte av å være en del av et nettverk som deler informasjon og hvor de kan treffe andre virksomheter i samme bransje og på denne måten få kunnskap om digital sikkerhet. De fleste har et håp om at de på sikt kan få gode råd også fra politiet, for eksempel gjennom næringslivskontakter. Selv om virksomhetene jobber mye med dette selv, ser de stor nytte i at politiet deler av sin kunnskap og erfaring.

4.2.1.4 Ledelsen

I utvalg 2 er det flere av informantene som trekker inn ledelsen i virksomhetene som et viktig element når det kommer til det digitale sikkerhetsarbeidet. Dette gjelder både når det skal besluttes hvorvidt informasjon skal deles med politiet, eller ikke, hvordan en hendelse skal

håndteres og hvor mye ressurser, tid og fokus sikkerhetsarbeidet i virksomheten skal få. Her kommer også modenhet inn, både når det kommer til ledelsen og virksomheten, og dette hører på mange måter sammen. I utvalg 2 forteller noen av informantene om at politiet kan bidra til å gi ledere i virksomheter økt kunnskap og forståelse for hvilken trussel virkosmhetene er utsatt for når det kommer til datakriminalitet. Kommunikasjon og fokus på kunnskap rettet mot lederne i virksomhetene vil kunne bidra til et bedre samarbeid med politiet.

> I en privat virksomhet er det ofte en toppledelse og et styre som naturlig nok vil ta avgjørelsen om å kontakte politiet, og om de skal gå ut med informasjonen eller ikke. Det kan det jo hende man aldri har trent på dette før eller diskutert scenariet tidligere, at man møter situasjonen helt uforberedt. Og at ledelsen rett og slett ikke har innsikt i eller kunnskap om og at de heller bare instinktivt tenker at dette sier vi ikke noe om før vi eventuelt må, og hvis noen spør er vi mest mulig ulne for dette går sikkert over av seg selv. De forstår rett og slett ikke konsekvensen av det. Dette gjelder nok en del virksomheter, at man egentlig aldri har diskutert temaet eller scenarioet, dette er bare noe som skjer med andre, eller at dette er noe som skjer nede hos IT-avdelingen (Sondre, Privat sikkerhetsselskap).

I utvalg 1 kommer det også frem at ledelsen har stor påvirkning når det kommer til hvordan virksomheten jobber med sikkerhet. Dette handler både om hvor mye fokus, tid og ressurser det digitale beredskapsarbeidet får, men også hvordan de som jobber med sikkerhet blir sett på dersom det går galt. Flere av informantene i utvalg 1 forteller at de fort ender «mellom barken og veden» når det kommer til å drive sikkerhetsarbeidet. På den ene siden får de lite oppmerksomhet og fokus fra ledelsen i det daglige når driften går som normalt, men når det skjer en uønsket hendelse får de fort veldig mye oppmerksomhet. Dersom virksomheten blir utsatt for alvorlig datakriminalitet hender det at de kjenner på en usikkerhet rundt det å kontakte politiet fordi de ikke ønsker at etterforskingen eller involveringen av politiet skal avdekke dårlig sikkerhet, i tillegg til at det kan bli sett på som negativt hos ledelsen. Dette varierer mellom virksomhetene, men det viser viktigheten av at sikkerheten forankres i ledelsen. Flere av informantene i utvalg 1 trekker også frem at kompetanseheving når det kommer til digital beredskap hos lederne har fått positiv effekt. Bevissthet hos lederne gjør at samarbeidet om sikkerhet i virksomhetene blir enklere og det danner grunnlaget for en mer helhetlig tilnærming. Dersom ledelsen går foran i jobben med digital sikkerhet er det enklere å få med hele virksomheten og dra lasset sammen mot en bedre digital sikkerhetskultur. Noen av informantene forteller også om ledere som har virkelig har forstått hvilken trussel

datakriminalitet og annen aktivitet på den digitale arena utgjør, noe som har gjort at sikkerhetsarbeidet får høy prioritet. Noen av virksomhetene har også lagt inn egne elementer for lederne når de trener og øver på for eksempel et dataangrep.

4.2.1.5 Helhetlig tilnærming og samfunnsansvar

Et aspekt av det som informantene kaller for modenhet er hvorvidt virksomhetene evner å løfte blikket og se på det å dele informasjon med politiet som et bidrag til en helhet og som et samfunnsansvar. I utvalg 2 er det flere av informantene som har sett eksempler på at virksomheter som både deler og som holder tilbake informasjon. I utvalg 1 er det forskjellige tanker og holdninger rundt dette, men flesteparten av informantene forteller at deres virksomhet er opptatt av samfunnsansvaret som ligger i å dele informasjon om datakriminalitet. De ønsker å bidra til en større helhet og ser nytten i å dele og tenke langsiktig. Det er ikke sikkert at virksomhetene vil se en umiddelbar effekt dersom de velger å dele informasjon om for eksempel et dataangrep, men det handler om å se at informasjonen kan komme noen andre til gode. Og neste gang kan det kanskje være omvendt når noen andre deler. På denne måten blir det å dele informasjon med politiet og legge seg på en åpen linje noe som kan bidra til virksomhetens sikkerhet. Flere av informantene fra begge utvalgene trekker også frem hvordan det kan være forskjeller mellom de store og de litt mindre virksomhetene når det kommer til å ha en helhetlig tilnærming. Kristoffer fra politi- og lensmannsetaten forteller om et konkret eksempel hvor informasjon fra en virksomhet bidro til at politiet fikk avverget en situasjon som raskt kunne ha utviklet seg til å bli veldig alvorlig.

> Det er nettopp fordi virksomhetene deler informasjon at vi kan fatte tiltak. Hvis virksomhetene ikke deler, og tenker at det sikkert er noen andre som gjør det, dersom alle tenker sånn så får ikke vi muligheten til å varsle virksomheten tidlig. Vi hadde nettopp en sånn sak hvor angriperne var inne i systemet til en virksomhet, men de hadde ikke kommet til den delen enda hvor de krypterer. Og da fikk vi sagt ifra på grunn av at andre virksomheter hadde varslet oss. Så virksomhetene må tenke større, at de har et ansvar for seg selv og sine interessenter, men også nasjonalt for deres konkurrenter. Så insentivet bør være at man får forebygget nye angrep og at man vil få igjen «tjenesten» på et tidspunkt hvis alle kan begynne å tenke sånn (Kristoffer, Politi- og lensmannsetaten).

I utvalg 1 forteller flere av informantene om at det som et utgangspunkt er stor villighet hos virksomhetene til å dele informasjon med politiet. De opplever at situasjonen slik den har

utviklet seg med trusselen fra datakriminelle og andre aktører som opererer i det digitale domenet har gjort at alle må stå sammen. Likevel er det noen ganger de opplever utfordringer innad i egen virksomhet når det kommer til holdninger og tilnærminger til hvordan man håndterer informasjonen og hvem man involverer, eventuelt ikke involverer. Ruben, fra politi- og lensmannsetaten, mener at det skjedde mye etter at Hydro valgte å være åpne om dataangrepet som rammet dem. Det viser at det hjelper at noen går foran, og han omtaler det som en «game changer». Likevel er det fremdeles en jobb å gjøre.

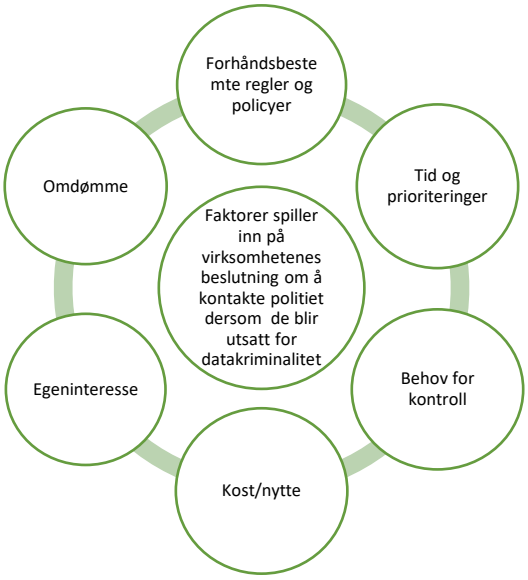
Oppsummering virksomhetenes digitale beredskapsarbeid

Det er tydelig blant informantene fra begge utvalgene at virksomhetenes beredskapsarbeid er helt sentralt når det kommer til samarbeid med politiet i forbindelse med datakriminalitet. Dette gjelder både mindre alvorlige forhold og alvorlige hendelser. Det kommer tydelig frem at arbeidet med digital beredskap er sentralt når det kommer til hvordan virksomhetene ser på datakriminalitet og hvordan modenheten til virksomhetene spiller inn på samarbeidet med politiet. Informantene fra begge utvalg trekker frem viktigheten av gode forberedelser, trening og øvelser, strategisk krisekommunikasjon og at sikkerhetsarbeidet forankres i ledelsen. De fleste av informantene fra utvalg 1 forteller at deres virksomhet ønsker å bidra i arbeidet med datakriminalitet gjennom informasjonsdeling og samarbeid med politiet, og de ser på dette som et bidrag i «dugnaden». Å ha en helhetlig tilnærming til datakriminaliteten og ta et samfunnsansvar er viktig i dette arbeidet, og informanter fra utvalg 2 forteller om at dette er sentralt for politiets arbeid med forebygging og håndtering av datakriminalitet. Det er ikke sikkert at politiet kan hjelpe virksomheten dersom de har vært uheldige, men informasjonen kan bidra til å avverge at det samme skjer med andre. Videre er informantene i utvalg 1 opptatte av at politiets deling av informasjon, kunnskap og erfaring kan spille dem gode i sikkerhets- og beredskapsarbeidet.

4.2.2 Faktorer som spiller inn på virksomhetenes beslutning om å kontakte politiet

Denne underkategorien omfatter flere faktorer som spiller inn på virksomhetenes beslutning om å kontakte politiet dersom virksomheten blir utsatt for datakriminalitet. Selv om flere av informantene i utvalg 1 fortalte at det å kontakte politiet dersom de blir utsatt for datakriminalitet, spesielt alvorlig datakriminalitet, gjerne var en sentral del av beredskapsplanene, kom det likevel frem at det gjøres en del situasjonsbestemte vurderinger i det enkelte tilfellet rundt det å kontakte politiet. Disse faktorene vil kunne påvirke om

virksomheten faktisk går til steget og kontakter politiet eller ikke. Intervjuobjektene ble stilt et åpent spørsmål som for å gå i dybden av disse faktorene. I løpet av prosessen med intervjuene kom det tydelig frem at informantene hadde tanker rundt mange av de samme faktorene, men gjerne med forskjellig vinkling. De to intervjuutvalgene hadde også interessante svar som både var sammenfallende og motstridende. Figur 4.8 viser de forskjellige faktorene som spiller inn på vurderingen om å kontakte politiet dersom virksomheten blir utsatt for datakriminalitet.



Figur 4.8 Underkategorier andre linje - Faktorer spiller inn på virksomhetenes beslutning om å kontakte politiet hvis/når de blir utsatt for datakriminalitet

4.2.2.1 Forhåndsbestemte regler og policyer

Flere av informantene i utvalg 1 fortalte om hvordan kontakt med politiet er en forhåndsbestemt del i beredskapsplanene. De kaller dette «regler om åpenhet», «policy», «rutiner» og «nulltoleranse». Samtidig som flere av informantene forteller om at det å kontakte politiet dersom de hadde blitt utsatt for datakriminalitet hadde vært helt naturlig for deres virksomhet og at dette «bare skjer automatisk», kom det også frem gjennom intervjuene at virksomhetene likevel ønsker å se an den enkelte situasjonen. Et eksempel på dette er den opplevde alvorlighetsgraden av hendelsen. Dersom virksomheten ikke opplever hendelsen som så alvorlig kan dette påvirke hvorvidt virksomheten faktisk kontakter politiet eller ikke.

Flere informanter i utvalg 1 jobber for store selskaper som igjen har flere underselskaper. De forteller at selv om selskapet de er en del av har regler og policyer om å kontakte politiet er det ikke alltid de opplever at dette er så enkelt å få gjennom hos underselskapene. De må ofte gå inn og gi dem råd og hjelpe dem med anmeldelsen og lignede

dersom det er behov for det. Det samme gjelder for kunder. Dette viser hvordan virksomhetene også er knyttet sammen med andre, enten kunder, underselskaper eller lignende og at en policy gjerne må etableres i flere ledd. Informantene knytter dette til arbeid med holdninger og sikkerhetskultur og viktigheten av en helhetlig tilnærming hos alle aktørene.

I utvalg 2 forteller flere av informantene at dersom myndighetskontakt og kontakt med politiet blir innlemmet i beredskapsplanene er det ofte en fordel med tanke på hva som faktisk gjøres når virksomhetene først har vært uheldige. De knytter dette til viktigheten av forberedelser. Likevel er opplevelsen til flere av informantene i utvalg 2 at ikke alle virksomheter følger policyene og at det gjøres situasjonsbestemte vurderinger i det enkelte tilfellet. Hvordan virksomhetene forholder seg til beredskapsplanverket og policy varierer fra virksomhet til virksomhet, og informantene mener at dette til syvende og sist handler om modenhet.

4.2.2.2 Egeninteresse – kost/nytte – tid og prioriteringer

Informantene fra utvalg 1 forteller alle om vurderinger som gjøres knyttet til tid, prioriteringer, kost/nytte og egeninteresse. Dette dreier seg både om den mindre alvorlige datakriminaliteten og alvorlig datakriminalitet, som for eksempel et dataangrep. Når det kommer til tid og prioriteringer forteller flere av informantene om at enkelthet og tilgjengelighet for kontakt med politiet er sentralt. Det er flere som trekker frem dette med hvordan prosessen med anmeldelser er hos politiet, og at det er lite aktuelt å dukke opp på et publikumsmottak for å levere en anmeldelse fysisk. Dette går tilbake til ønsker om å få på plass en digital løsning for anmeldelser. Flere av informantene har fått med seg politiets tips-funksjon og synes at dette er et steg i riktig retning. Også her blir næringslivskontaktene et sentralt tema fordi informantene opplever dette som et tiltak som gjør det enklere for dem å kunne kontakte politiet i forbindelse med datakriminalitet. De trekker alle frem at det må være enkelt å kontakte politiet, og det er en fordel dersom de vet at de kommer frem til polititjenestepersoner med riktig kompetanse og muligheten til å hjelpe virksomhetene.

Når det gjelder tid og prioriteringer handler dette om håndteringen av en krise dersom virksomheten blir utsatt for alvorlig datakriminalitet. Informanter fra utvalg 1 forteller om at det i den innledende fasen av en krise, da det også er viktig å involvere politiet raskt, vil være mange arbeidsoppgaver og en kaotisk situasjon. Å kontakte politiet i en slik setting, dersom man vurderer at det ikke kommer til å bidra i hendelseshåndteringen, vil gjerne havne lengre

ned på prioriteringslisten over ting som skal gjøres. Her er virksomhetenes opplevelse av politiets kunnskap og kompetanse når det kommer til datakriminalitet sentralt, i tillegg til virksomhetenes kunnskap om hva politiet kan bidra med. Likevel trekker de informantene fra utvalg 1 som jobber for en virksomhet som har blitt utsatt for alvorlig datakriminalitet og har erfaring fra samarbeid med politiet frem at denne erfaringen var såpass positiv at dette vil stå høyt opp på prioriteringslisten dersom virksomhetene skulle bli utsatt for alvorlig datakriminalitet igjen. Et annet moment når det gjelder prioriteringer er at dersom virksomheten blir utsatt for alvorlig datakriminalitet som truer virksomhetens eksistens, kan det hende at kontakt med politiet blir nedprioritert i arbeidet med å redde virksomheten.

Videre nevner flere av informantene i utvalg 1 egeninteresse når det kommer til å kontakte politiet. Dette handler om å få noe igjen, altså at politiet kan tilby noe tilbake til virksomhetene. Dette kan handle om å få råd og hjelp i hendelseshåndteringen. Flere gir uttrykk for at de ikke nødvendigvis har forventninger til at politiet kan løse den situasjonen de står i, men de ønsker likevel å få råd og veiledning til hvordan de best kan løse situasjonen og få dra nytte av politiets kunnskap og erfaring når det kommer til å håndtere datakriminalitet. Å få noe tilbake kan også dreie seg om den mindre alvorlige datakriminaliteten og informasjonen virksomhetene deler med politiet.

> Det første som slår meg når vi snakker om informasjonsdeling er «toveis». At vi ikke øser over alt vi har også får vi ingenting tilbake. Det vil være utfordrende og det vil ikke stimulere til samarbeid. Og det er «sammen» som er greia her og involvering. Vi må få noe igjen for det vi deler. Vi kan ikke da få beskjed om at politiet ikke kan dele fordi det er etterforskning osv., det «flyr ikke». Vi er store på sikkerhet og vi tar det seriøst og har et stort samfunnsansvar, så vil jo vi dele vi uansett hva vi får vi får tilbake. Men det vil likevel være mye mer nyttig, effektivt og gledelig å få noe tilbake (Ole Gunnar, Finans).

Informanter fra utvalg 2 forteller at de opplever at en av de viktigste årsakene til at virksomhetene kontakter politiet er for å få råd og hjelp til å løse en krisesituasjon. I en slik setting kan det også oppstå utfordringer rundt samarbeidet, åpenhet og informasjonsdeling fordi virksomhetene kanskje er usikre på hva de får igjen dersom de åpner opp om det som har skjedd. Harald, fra et offentlig myndighetsorgan, forteller om situasjoner hvor han har blitt kontaktet av virksomheter som har blitt utsatt for alvorlig datakriminalitet, hvor virksomheten er tilbakeholden med å dele informasjon. I slike situasjoner har han vært opptatt av å forklare virksomhetene at dersom de deler informasjon kan det hende at myndighetene

kan sette informasjonen i kontekst, noe som gjør at virksomheten kan få hjelp gjennom at myndighetene vet noe om aktørene eller lignende, eller at det kan fremkomme annen informasjon som kan hjelpe virksomheten med hendelseshåndteringen for eksempel med å begrense skader. Informanter med tilknytning til politi- og lensmannsetaten fortalte informasjon fra virksomhetene, enten det gjelder mindre alvorlig eller alvorlig datakriminalitet, vil kunne sette politiet i bedre stand til å gi noe tilbake, og det politiet har som mål å komme dit at kunnskapsgrunnlaget og det internasjonale samarbeidet skal bidra til at politiet kan gi noe tilbake til virksomhetene. Videre vil økt kunnskap og kompetanse i politiet kunne bidra til bedre rådgivning og hjelp i alvorlige situasjoner, men også i det daglige.

4.2.2.3 Omdømme og behov for kontroll

I utvalg 2 forteller flere av informantene at de opplever at virksomhetenes åpenhet og modenhet som noe som er nært knyttet til virksomhetens omdømme. Informantene har flere eksempler på virksomheter som har hold dataangrep skjult, noe som både kan handle om at virksomhetene er flaue over dårlig sikkerhet eller at de er redde for at dersom informasjonen kommer ut vil dette kunne påvirke virksomhetens omdømme negativt og ha konsekvenser for virksomhetens drift. Likevel peker flere av informantene i utvalg 2 på at virksomheter som velger å være åpne og som velger å dele informasjon med politiet ofte kommer veldig bra ut av en krise. Måten Hydro valgte å legge seg på en åpen linje da de ble utsatt for et dataangrep i 2019 trekkes frem som et eksempel på at omdømmet til virksomheten ble bevart til tross for at de hadde blitt angrepet og de delte informasjon om dette. Når informantene i utvalg 2 snakker om omdømme trekkes dette ofte frem som en faktor som gjør at virksomhetene lar være å kontakte politiet og være åpne om hendelsen dersom de ikke må. Patrick, fra et privat sikkerhetsselskap, trekker imidlertid frem et annet aspekt rundt dette med åpenhet, som også går igjen i det informantene fra utvalg 1 forteller om.

> Jeg tror det er viktig å spille på åpenhet for jeg tror det kan gjøre noe positivt med omdømmet. For en stund tilbake ble et verft på Vestlandet utsatt for et dataangrep. Verftet opplevde at å velge en åpen linje gjorde noe med virksomhetens kultur og virksomheten ble møtt med forståelse i markedet og holdninger som «dette kan skje alle, flott at dere går ut og forteller om det». Tilliten økte. En annen virksomhet innen teknologi og innovasjon hadde fortalt det samme. De har vært åpne om dataangrep flere ganger og har fortalt at åpenhet gjør noe med trusselaktøren og det gjør noe med

> tilliten og kunnskap i samfunnet. Det å være åpen også kan være positivt, altså at du vise sårbarhetene dine og at virksomheten tar situasjonen på alvor. Suksesskriteriet i dette er god krisekommunikasjon (Patrick, Privat sikkerhetsselskap).

Noen av informantene i utvalg 2 forteller at de tror at dette med omdømme kan gå to veier når det kommer til samarbeid med politiet. Noen virksomheter vil ønske å ikke dele informasjon og være åpne fordi de tenker at det vil kunne svekke omdømmet gjennom at for eksempel dårlig datasikkerhet kanskje vil bli avslørt, mens andre involverer politiet helt bevisst for å styrke omdømmet og vise at de tar situasjonen seriøst og ønsker å bidra til å bekjempe datakriminalitet, og noen fordi de trenger hjelp. I noen tilfeller kan det også tenkes at virksomhetene kanskje vurderer hvorvidt de må være åpne om et angrep, og at usikkerhet er et moment når det kommer til virksomhetens vurdering om å være åpen og involvere myndighetene i en tidlig fase av krisen.

> Det vil være en forskjell på hva man må gjøre og hva det er lurt å gjøre. Selvfølgelig er det ett poeng som går på usikkerhet om hva som skjer hvis man anmelder forholdet og om det er noen vits i å gjøre det. Det er nok mange virksomheter som ønsker å være åpne, men så er det en så tidlig fase at man ikke vil tilkjennegi det før man har mer kontroll. I tillegg kan det være ønske om å involvere så få som mulig, slik at det ikke blir offentlig kjent. Virksomheter er redd for sitt eget omdømme og hva slags betydning dette vil kunne ha for virksomheten. Derfor er det viktig at virksomheter har tillit til at offentlige myndigheter kan ivareta ulike interesser og behov som virksomheter har (Harald, Offentlig myndighetsorgan).

Flere av informantene i utvalg 1 forteller om å snu dette med omdømme til noe positivt, og at det å kontakte politiet i dag ofte heller blir sett på som at virksomheten er moden og tar utfordringene med datakriminalitet og trusler fra det digitale rom på alvor. Dette har for mange virksomheter handlet om å snu holdningene til dette og vise at det ikke er skadelig å være åpen. Dersom man velger å ikke involvere politiet i dag kan det fort gjøre at virksomheten oppfattes som useriøs og lite profesjonell. Ole Gunnar fra Finans forteller at hans virksomhet må være åpen og involvere politiet nettopp for å verne om omdømmet, for det er viktig å vise at de er en seriøs og «ryddig» virksomhet. Også Stian fra Teknologi og innovasjon forteller om viktigheten av å være åpne:

> For det første så er det grunnleggende viktig for oss å fremstå som en seriøs samfunnsaktør, noe som vil si å bidra til det vi mener er viktig i samfunnet, og åpenhet er viktig i samfunnet. Det er en helt grunnleggende holdning hos oss, og det

> harmonerer med verdisettet vårt. Så jeg kan ikke forestille meg at vi skulle forsøke å legge lokk på den type informasjon fordi det der er typisk en sånn sak som kommer og slår deg etterpå, så det er mye bedre å være åpen om det. Vi har hatt ett tilfelle i løpet av de siste årene der det viste seg at vi var hacket. Åpenheten vår ga oss ekstremt positiv feedback av alle kundene som var involvert i det. Så vår erfaring er at når sånt skjer må du være åpen og proaktiv i stedet for å håpe at kanskje noen ikke oppdager det så det går over (Stian, Teknologi og innovasjon).

Flere av informantene i utvalg 1 trekker også frem at det å være redd for at åpenhet og det å involvere politiet kanskje skal skade omdømmet ikke gjelder like mye lenger. Dette handler mulig om at flere virksomheter har vært åpne noe som er med på å senke terskelen for andre, i tillegg er det så vanlig at virksomheter på ett eller annet tidspunkt blir utsatt for alvorlig datakriminalitet og man ser at metodene som brukes av de kriminelle aktørene er så profesjonelle og sofistikerte at det ikke alltid handler om hvor gode tekniske sikkerhetsløsninger en virksomhet har eller hvor godt organisert man er. Dersom de kriminelle er gode nok, kommer de seg inn. Så det gjelder heller å spille hverandre gode gjennom å dele informasjon. Det å anmelde datakriminalitet til politiet blir også sett på av noen av informantene i utvalg 1 som noe virksomhetene gjør for å ha «ryggen fri», altså at de anmelder for da har de gjort sin del, da kan ingen ta dem for at de ikke gikk til politiet, noe også noen av informantene i utvalg 2 forteller om.

Når det kommer til omdømme forteller informantene fra begge utvalg også om hvordan det personlige omdømmet til de personene som sitter i sentrale sikkerhetsstillinger i virksomhetene, for eksempel i rollen som CISO, kan påvirkes. Dersom ikke sikkerhet i virksomheten er godt forankret i ledelsen og ledelsen forstår viktigheten av å fokusere på og prioritere arbeidet med beredskap og digital sikkerhet, vil de personene som har dette ansvaret kunne møte en del motstand i det daglige fordi det er vanskelig å få gjennomslag for sikkerhetsløsninger, trening osv., samtidig vil de samme personene raskt kunne «få skylden» dersom det går galt og virksomheten blir utsatt for alvorlig datakriminalitet. Noen av informantene i utvalg 1 forteller om en usikkerhet og en dårlig mageføelse når det kommer til å sitte med mye ansvar når det kommer til arbeidet med digital sikkerhet. Usikkerheten knytter seg til hva de vil oppleve dersom det går galt en dag. Kristoffer, fra politi- og lensmannsetaten, trekker frem at dersom en CISO eller en annen person som er ansvarlig for den digitale sikkerheten i en virksomhet kjenner mye på usikkerhet rundt hvordan vedkommende blir ansett dersom det går galt i en virksomhet, kan dette være med på å

vanskeliggjøre kommunikasjonen og informasjonsdelingen med politiet. For det er ofte denne personen som også sitter sentralt i dette samarbeidet.

Flere av intervjuobjektene i utvalg 1 forteller at de har policyer om å kontakte politiet og de har diskutert hvordan og når dette skal gjøres med ledelsen. Det er vanskelig å lande på en standard som alltid skal følges uansett. For flere av virksomhetene til informantene er dette noe som vurderes i det enkelte tilfellet. De forteller også om et behov for å ha kontroll på situasjonen før de kan vurdere å gå til politiet. I utvalg 2 nevner noen av informantene at virksomhetene mulig opplever at de mister handlingsalternativene sine i en hendelse dersom de kontakter politiet. Naturlig nok vil virksomhetene prioritere å gjenoppta sikker drift av selskapet og i noen tilfeller vil kanskje noen velge å for eksempel betale et løsepengevirus for å nettopp få opp produksjonen igjen. Intervjuobjektene forteller også om virksomheter som har kontaktet politiet etter at de har betalt fordi det ikke ga det resultatet de ønsket. Informanter fra utvalg 2 håper at virksomhetene vil komme til politiet, fordi politiet kan gi dem god beslutningsstøtte i de valgene de står ovenfor. Et eksempel på dette er at de datakriminelle har kjørt noe som kalles «dobbel utpressing», hvor virksomheten kanskje betaler, med de datakriminelle forblir i nettverket og presser virksomhetene for mer penger. Dette er informasjon politiet kunne gitt flere virksomheter underveis i hendelseshåndteringen dersom politiet hadde blitt involvert.

Informanter fra begge utvalg forteller om at virksomhetene har en kompleks målgruppe å forholde seg til, noe som kan spille inn på hvordan virksomheten håndterer datakriminalitet og involvering av politiet. Informanter fra utvalg 1 trekker inn at det er viktig for dem å kunne samarbeide med politiet uten at informasjonen lekker og det blir gjort til noe større enn det trenger å være, noe som i ytterste konsekvens kan føre til at en virksomhet mister viktige kontakter og relasjoner. Flere av informantene fra utvalg 1 trekker frem at man ikke ønsker å bekymre stakeholderne unødig, spesielt i en innledende fase av en hendelse eller krise når det er mye usikkerhet. Flere av informantene forteller om behovet for å styre den informasjonen som kommer ut og når den kommer ut. De trekker frem at det er veldig viktig for virksomhetene at politiet har respekt for dette behovet. Kåre fra matproduksjon forteller at da hans virksomhet ble utsatt for et dataangrep utfordret de politiet helt eksplisitt på dette for at de skulle få de forsikringene de trengte. Dette dannet grunnlaget for et godt samarbeid gjennom hendelseshåndteringen.

Flere av informantene med tilknytning til politi- og lensmannsetaten forteller at holdninger og antakelser hos virksomhetene som for eksempel at det å involvere politiet er

ensbetydende med at informasjonen blir offentlig kjent og at det kommer ut at virksomheten har blitt utsatt for noe kan komme i veien for et godt samarbeid. Informantene i utvalg 1 forteller at det er helt avgjørende i samarbeidet med virksomhetene at politiet og myndighetene har et godt tillitsforhold med virksomhetene og at politiet tar hensyn til virksomhetenes behov for kontroll over informasjonen.

Oppsummering faktorer som påvirker virksomhetenes beslutning om å kontakte politiet dersom de blir utsatt for datakriminalitet

Selv om mange av virksomhetene som informantene i utvalg 1 er knyttet til har beredskapsplaner og policyer som tilsier at de skal kontakte politiet, er det flere faktorer som til syvende og sist spiller inn på disse vurderingene. Det er et komplekst bilde med flere hensyn som skal tas, og det varierer hvordan virksomhetene vurderer de forskjellige faktorene. Dette handler i all hovedsak om forhåndsbestemte regler og policyer, behovet for å gjøre situasjonsbestemte vurderinger, kost/nytte, egeninteresse, tid og prioriteringer, virksomhetens omdømme, komplekse målgruppe og behov for kontroll i en kaotisk situasjon. Utvalg 2 forteller at selv om mange av virksomhetene har kommet langt i arbeidet med beredskap og forholder seg til datakriminalitet på en helhetlig og samfunnsansvarlig måte, opplever de at mange virksomheter uansett situasjon har et behov for kontroll og vil vurdere hver situasjon for seg. Spesielt informantene som er knyttet til politi- og lensmannsetaten håper at virksomhetene vil delta i «dugnaden» slik at politiet kan utøve sin rolle når det kommer til datakriminalitet.

4.2.3 Virksomhetenes relasjon til politiet – erfaringer og forventninger

Gjennom intervjuene fortalte informantene fra utvalg 1 om både erfaringer fra møtet med politiet, både i forbindelse med henvendelser gjeldende datakriminalitet og ellers, i tillegg til deres forventninger. Det var flere av informantene som hadde opplevd negative møter med politiet, samtidig som at de som hadde erfaring fra samarbeid med politiet ofte hadde positive opplevelser. Informantene fortalte også om forventninger i denne sammenheng.

4.2.3.1 Erfaringer fra møte med politiet

I utvalg 1 forteller flere av informantene om negative opplevelser fra møter med politiet i forbindelse med datakriminalitet. Eksempler på slike negative opplevelser er at politiet ikke har tatt imot informasjonen virksomheten har kommet med, manglende kompetanse og kapasitet har gjort at noen har opplevd å ikke bli tatt imot i det hele tatt og noen har opplevd

dårlige holdninger og fordommer mot virksomhetene fra politiansatte. Dette beskriver informantene som svært skadelig for tilliten til politiet og det vil i kunne påvirke samarbeidet mellom virksomhetene og politiet. Når det kommer til datakriminalitet og en hendelse som for eksempel et dataangrep ønsker virksomhetene å treffe på politifolk med kompetanse og som kan gi dem god råd og støtte i hendelseshåndteringen. Andreas fra teknologi og innovasjon forteller at han har opplevd politifolk som i møte med virksomheten hans har forklart at det er umulig å etterforske en sak fordi gjerningspersonene hadde benyttet relativt vanlig og enkle sikkerhetstiltak for å skjule seg på nett. Andreas forteller at han jobber i en virksomhet hvor de har en veldig kompetent IT-avdeling, som visste godt at det overhodet ikke var umulig å etterforske. Han forstod at denne uttalelsen fra politiet mest sannsynlig bunnet i kompetanse og kapasitet, men han etterlyser en mer profesjonell fremtreden i møte med virksomhetene, og at politiet også kan vise ydmykhet for at mange virksomheter har høyt kompetente folk. Man blir fort gjennomskuet dersom man ikke klarer å være ærlig om manglende kompetanse og heller velger en unnskyldning. Informanter fra utvalg 2 forteller at virksomhetene vil kunne bli møtt veldig forskjellig med bakgrunn i det varierende kompetanse- og kapasitetsnivået i norsk politi når det kommer til datakriminalitet.

4.2.3.2 Erfaringer fra samarbeid med politiet

Informantene fra utvalg 1 som har erfaring fra samarbeid med politiet i forbindelse med datakriminalitet forteller om positive opplevelser. De fortalte også at holdningene deres og synet på samarbeid med politiet endret seg i etterkant av samarbeidet. De positive opplevelsene knytter de til at politiet ga dem god støtte i håndteringen av krisen og at politiet delte informasjon som var nyttig i beslutningstakingen. I utvalg 2 forteller informantene om viktigheten av å etablere gode tillitsforhold til virksomhetene både før, under og etter en hendelse. Dette ser de på som et kontinuerlig arbeid som må skje i hele politi- og lensmannsetaten. Videre er de opptatte av å ta hensyn til virksomhetene og den situasjonen de står i med tanke på trusselen fra datakriminelle og andre aktører i det digitale domenet. Her handler det også om skape trygghet slik at virksomheter som kanskje ikke har gjort en like god jobb med beredskapsarbeidet opplever at de kan involvere politiet uten at dette skal bli en negativ opplevelse. Informantene med tilknytning til politi- og lensmannsetaten, ser hvor godt de nyter av virksomheter som har hatt gode opplevelser med samarbeidet og hvordan dette kan smitte over på andre. Flere av informantene i begge utvalg trekker frem viktigheten av at suksesshistoriene deles. Flere av informantene i utvalg 1 som jobber for virksomheter som ikke har opplevd en stor krise i forbindelse med datakriminalitet, har dratt læring av hendelsen

som rammet Hydro, og har fått opp øynene for den jobben politiet bidro med i den saken.

4.2.3.3 Forventninger til politiets arbeid med datakriminalitet

Det er varierende hvilke forventninger virksomhetene har til politiets arbeid med datakriminalitet nå og for fremtiden. De fleste informantene i utvalg 1 er usikre på hvilke forventninger det er realistisk å ha. Noe som gikk igjen hos flere av informantene var at de forventer at norsk politi evner å delta i internasjonalt politisamarbeid og at informasjonen virksomhetene kommer med blir koordinert og satt i en større kontekst. Videre ønsker informantene at politiet fortsetter satsningen på næringslivskontakter slik at de får en tettere kontakt med politiet og at terskelen for samarbeid blir lavere. Et viktig moment som også gikk igjen, var at det må etableres enklere og mer tilgjengelige løsninger for anmeldelser og deling av informasjon til politiet. Selv om informantene fra utvalg 1 kom med flere forventninger, var det flere av dem som heller ville fokusere på ønsker i stedet for forventninger. De fleste av informantene i utvalg 1 ønsker seg et politi som tar eierskap til tematikken og som inviterer til seminarer og andre arrangementer hvor politiet kan dele av sin informasjon, kunnskap og erfaring, og at dette kan føre til at virksomhetene får god veiledning når det kommer til å drive sitt sikkerhets- og beredskapsarbeid. Flere nevner også at de håper at politiet kommer dit at de evner å ta imot anmeldelser, tips og informasjon som virksomhetene besitter og forvalte dette på en god måte inn i det forebyggende arbeidet. Det er også et ønske at politiet skal kommunisere bedre til virksomhetene hvordan de jobber og tydeliggjøre rollen og mandatet, og synes mer i mediebildet. Flere av informantene forteller også at de ønsker å føle seg trygge på at når det virkelig går galt, kan de få gode råd og hjelp fra et politi som evner å respondere raskt og har den kompetansen som trengs. Gjennomgående forteller informantene i utvalg 1 at de ønsker å dele informasjon med politiet og bidra til arbeidet med datakriminalitet.

Samtidig som informantene i utvalg 1 har mange forventninger og ønsker når det kommer til hva politiet skal klare å levere når det kommer til forebygging og håndtering av datakriminalitet, forteller de også om ønsker og forventninger til egen virksomhet og næringslivet ellers. De ønsker at virksomhetene jobber med beredskapsarbeid knyttet til datakriminalitet og trusselen fra andre aktører på digital arena slik at virksomhetene kan dra nytte av hverandres opplevelser. Flere erkjenner at de har en vei å gå med beredskapsarbeidet og å sette seg bedre inn i tematikken. I tillegg peker de på viktigheten av at alle må tenke mer langsiktig og de stiller seg positive til det informantene i utvalg 2 har omtalt som «dugnad»,

altså at de kan dra nytte av hverandre og at alle deler informasjon og er åpne om hendelser til politiet.

> Det som kan bli bedre, og jeg tror ikke dette nødvendigvis bare må legges på politiet og NSM alene, det handler om å forebygge datakriminalitet. Selv om vi har trent og har beredskapsplaner og kontinuitetsplaner i virksomheten, så er et hackerangrep en høyst teoretisk problemstilling før det treffer. Det er som en frontkollisjon, og det er enkelt å tenke «det skjer ikke oss». Det kan fungere som en barrierebygger med tanke på det forebyggende arbeidet. Så det å ha bevissthet rundt at det høyst sannsynlig kommer til å skje på ett eller annet tidspunkt, hvertfall for de større virksomhetene, det tror jeg er et viktig punkt som krever at næringslivet, politiet, NSM og myndighetene ellers samarbeider og løfter dette som en relevant problemstilling for alle (Kåre, Matproduksjon).

Også utvalg 2 forteller om både forventninger og ønsker når det kommer til politiets arbeid med datakriminalitet og hva som kan gjøres for å legge bedre til rette for et godt samarbeid. Flere av informantene nevner at politiet bør bli flinkere til å nyttiggjøre seg av «solskinnshistoriene» og vise frem i media det arbeidet som gjøres når det kommer til datakriminalitet. Det er også ønskelig at politiet skal ta mer eierskap til mandatet sitt og ta en mer aktiv rolle i samfunnsdebatten. Å være mer synlig utad handler om å bygge tillit til næringslivet over tid. Videre nevner flere av informantene i dette utvalget at det må skje en kompetanseheving når det kommer til datakriminalitet i hele politiet, noe som krever at politiledelsen tar tak. Politiet ville også vært tjent med å kommunisere til næringslivet og samfunnet hvilken rolle politiet har når det kommer til datakriminalitet, hva politiet ønsker av informasjon, hvordan informasjonen brukes og hvordan politiet ligger an i arbeidet med datakriminaliteten. Det jobbes med å etablere et bedre mottaksapparat for informasjon og anmeldelser, og de informantene som er tilknyttet politi- og lensmannsetaten håper at politiet i større grad klarer å forvalte og benytte denne informasjonen aktivt i det forebyggende arbeidet i fremtiden.

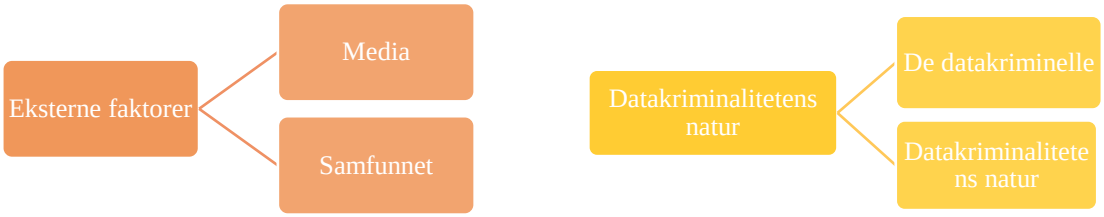
Oppsummering virksomhetenes relasjon til politiet

Flere av informantene i utvalg 1 har negative erfaringer fra møter med politiet, noe som mulig kan ses i sammenheng med usikkerhet og lav kompetanse flere steder i politiet når det kommer til datakriminalitet. Dette er også noe informantene i utvalg 2 vet at skjer. Samtidig trekker mange av informantene i utvalg 1 frem at de har gode erfaringer fra samarbeid med

politiet, noe som har bidratt til å øke tilliten til politiets håndtering av datakriminalitet. Informantene i utvalg 1 har høye forventninger til politiets arbeid med datakriminalitet, samtidig som mange også forteller at de heller vil omtale det som ønsker med bakgrunn i at de ikke helt vet hva som er realistisk å forvente. Mange av forventningene og ønskene går i retning av å få på plass kompetanse og kapasitet slik at samarbeidet mellom næringslivet og politiet kan styrkes når det kommer til forebygging og håndtering av datakriminalitet. Flere av informantene i utvalg 1 trekker også frem at dette ikke er et ansvar som ligger på politiet alene, og at virksomhetene også må gjøre en jobb. Informantene i utvalg 2 fokuserer på at kompetansen og kapasiteten når det kommer til datakriminalitet må økes gjennomgående i politiet, og at politiet har mye å hente når det kommer til synliggjøring, eierskap og ekstern kommunikasjon. .

4.3 Datakriminaliteten, media og samfunnet

Denne hovedkategorien er en sammenslåing av «Eksterne faktorer» og «Datakriminalitetens natur». Disse to hovedkategoriene er mindre i innhold enn hovedkategori 2 og 3. Figur 4.9 viser en oversikt over hovedkategori 3 og 4 med underkategorier.



Figur 4.9 Oversikt over hovedkategori 3 «Eksterne faktorer» og hovedkategori 4 «Datakriminalitetens natur» med underkategorier første linje

4.3.1 Media og samfunnet

Flere av informantene i utvalg 1 forteller om hvordan medias fremstilling av alvorlige datasikkerhetshendelser, datakriminalitet osv. kan påvirke virksomhetens valg om åpenhet og samarbeid med politiet. Dette har bakgrunn i at informantene opplever at media påvirker samfunnets kunnskap, opplevelse av og holdninger til datakriminalitet, noe som legger føringer for hva samfunnet tenker om virksomheten dersom det kommer ut at virksomheten har blitt usatt for datakriminalitet. Informantene savner at media i større grad velger å fokusere på det positive dersom virksomhetene velger å være åpne i stedet for å henge ut virksomhetene for å for eksempel ha dårlig datasikkerhet. Flere av informantene i utvalg 1

forteller at de vet om mange virksomheter som har valgt å ikke være åpne, hverken i media eller til politiet. Flere påpeker at det er viktig å øke kunnskapen i samfunnet om hvor profesjonelle de datakriminelle er og at det ikke trenger å bety at en virksomhet har gjort en dårlig jobb med sikkerheten dersom de blir utsatt for et dataangrep eller lignende. Dette vil være viktig opp mot kundeforhold og omdømme også. Noen av informantene i utvalg 1 forteller også at de er opptatte av å bruke media for å være åpne for å opprettholde tillitsforhold til samfunnet.

> Jeg ser absolutt ulempene med å være åpen! Det er synd når noen i pressen går ut og «skyter på» en virksomhet fordi de ikke har vært gode nok og legger ut om at de kunne unngått det osv. Jeg tror man skal passe seg for å gå ut den veien, det er bedre å rose folk. Jeg tror ikke vi vil være i nærheten av å kunne fighte dette om vi ikke står sammen. Vi må tørre å være så åpne med hverandre og vi må komme til et nivå av tillit i samfunnet at det ikke er flaut å være åpne. Virksomhetene må kunne være sikre på at dersom de faktisk tørr å rekke opp hånden og si at det har skjedd oss så må de ikke bli skutt ned (Ola, Import og salg).

Informantene fra utvalg 2 trekker frem at politiet i større grad kan bli flinke til å bruke media som et talerør til samfunnet for å endre holdninger og antakelser rundt datakriminalitet, og samtidig heve kunnskapen i samfunnet når det kommer til fenomenet. Det vil også være viktig å vise politiets arbeid som en ren individuell- og allmennpreventiv effekt for å forebygge datakriminalitet. Flere av informantene i dette utvalget nevner også at de synes det er merkelig hvor lite oppmerksomhet alvorlig datakriminalitet får i samfunnet, og nevner her at media er viktig for at samfunnet skal få opp øynene og begynne å se hvor alvorlig trusselen fra datakriminelle faktisk er i dag. Dette vil kunne senke terskelen for virksomhetene til å velge åpenhet, fordi tabuet i samfunnet kan reduseres gjennom kunnskapsheving. I utvalg 2 trekker flere av informantene paralleller mellom virksomhetenes vurdering rundt omdømme og medias fremstilling av en hendelse. Virksomheten kan oppleve å miste kontroll hvis informasjon om alvorlig datakriminalitet lekker til media før virksomheten er klar for det.

4.3.2 Datakriminaliteten og de datakriminelle

Informantene i utvalg 1 forteller at de opplever datakriminalitet som et krevende felt. Dette baserer seg mye på at hurtig skiftende trusselbilde som det er vanskelig å ha oversikt over, en grenseoverskridende og global form for kriminalitet og at de kriminelle er så gode på det de driver med at virksomhetene fort kan føle på en slags håpløshet når det kommer til å skulle

drive sikkerhet- og beredskapsarbeid og hendelseshåndtering. De beskriver en følelse av at de kriminelle vil kunne klare å komme seg inn i systemene nesten uansett hvor god sikkerhet virksomhetene har, fordi de kriminelle også benytter seg av menneskelige feil og svakheter for å få tilgang til systemene. Dette er det flere av informantene i utvalg 1 som nevner i forbindelse med arbeidet med å etablere en god sikkerhetskultur, også digitalt, og det er viktig at de ansatte i virksomheten forstår hvordan de som enkeltindivider kan jobbe og bidra til virksomhetens sikkerhet. Videre forteller noen av informantene om at det bare er et spørsmål om tid før de fleste virksomheter har blitt utsatt for alvorlig datakriminalitet, og det er heller ikke sånn at dersom man har blitt utsatt en gang skjer det ikke igjen. De datakriminelle utvikler nye metoder og finner nye sårbarheter og smutthull hele tiden.

Harald, fra et offentlig myndighetsorgan, forteller om hvordan datakriminaliteten, spesielt når det kommer til løsepengevirus, har endret det digitale trusselbildet. Selv om kriminalitet i all hovedsak er politiets mandat, har plutselig datakriminaliteten blitt en trussel med store samfunnsmessige konsekvenser som også går over i mandatet til andre offentlige myndigheter. Han omtaler en enorm destruktiv effekt som kan få store konsekvenser i systemer og tjenester som samfunnet er helt avhengig av. Han forteller også hvordan metodene til de kriminelle utvikler seg og at de stadig finner nye metoder for å utnytte sårbarheter maksimalt. Dette kan for eksempel dreie seg om at de kriminelle aktørene er inne i virksomhetens systemer over lengre tid og henter ut sensitive opplysninger, bedriftshemmeligheter som de truer med å publisere.

Oppsummering datakriminaliteten, media og samfunnet

Flere av informantene i utvalg 1 forteller at datakriminaliteten og de datakriminelle utfordrer virksomhetenes arbeid med digital sikkerhet. Datakriminaliteten er global og grenseoverskridende, og de datakriminelle er profesjonelle og tilpasningsdyktige. Det er en rådende oppfatning om at dersom de datakriminelle vil komme seg inn i systemene til virksomheten så får de til det, uansett hvor god sikkerheten er. Dette er også noe informantene synes er viktig at kommer bedre frem i samfunnsdebatten, noe som kan bidra til å styrke samfunnets kunnskap om datakriminaliteten, og igjen senke terskelen for virksomhetene når det kommer til å velge en åpen linje og samarbeid med politiet og andre myndigheter. Begge utvalgene trekker frem at media har en sentral rolle når det kommer til å «utdanne» samfunnet, og politiet kan i større grad også benytte seg av disse kanalene.

4.4 Kobling mellom forskningsspørsmål og empiriske funn

Gjennom kapittel 4 har jeg oppsummert de empiriske funnene knyttet til de 3 hovedkategoriene «Politiet og datakriminalitet», «Virksomhetenes beredskapsarbeid» og «Datakriminalitet, media og samfunnet». I all hovedsak har empirien belyst menneskelige og organisatoriske faktorer som har positiv og negativ påvirkning på de de norske virksomhetenes samarbeid med politiet når det kommer til forebygging og håndtering av datakriminalitet. De menneskelige og organisatoriske faktorene treffer både virksomhetene og politiet. Tabell 4.2 viser koblingen mellom forskningsspørsmålene og de empiriske funnene.

Forskningsspørsmål	**Empiriske funn**
Hvordan påvirker politiets arbeid med datakriminalitet virksomhetenes samarbeid med politiet?	• Politiets kapasitet og kompetanse når det kommer til datakriminalitet påvirker tillitsforholdet mellom virksomhetene og politiet • Lav kapasitet og kompetanse over tid har gjort at andre, både offentlige og private aktører, har kommet på banen og tatt et rom og et ansvar som politiet burde tatt • Politiets satsning på datakriminalitet de siste årene gjennom etableringen av NC3 og satsing på næringslivskontakter blir sett på som et steg i riktig retning og vil kunne forbedre samarbeidet • Virksomhetene ønsker at politiet skal synes mer i samfunnsdebatten og ta mer eierskap til datakriminaliteten. Dette vil bidra til at politiet blir en mer aktuell aktør å samarbeide med, i tillegg til at virksomhetene vil få økt kunnskap om hva politiet kan bidra med • Politiet har en vei å gå når det kommer til å kommunisere til virksomhetene om hvilken informasjon politiet trenger og hvordan virksomhetene skal forholde seg til mindre alvorlig og alvorlig datakriminalitet • Virksomhetene ønsker at politiet i større grad skal bidra til virksomhetenes beredskapsarbeid gjennom å dele informasjon, kunnskap og erfaring knyttet til datakriminalitet • Politiet må etablere enklere og mer tilgjengelige løsninger deling av informasjon, samt et system for forvaltning av informasjonen inn i politiets kunnskapsgrunnlag
Hvordan påvirker virksomhetenes beredskapsarbeid samarbeidet med politiet?	• Gode forberedelser gjennom beredskapsarbeidet vil øke sjansen for et godt samarbeid mellom virksomhetene og politiet, både når det kommer til mindre alvorlig og alvorlig datakriminalitet • Sikkerhets- og beredskapsarbeidet bør forankres i virksomhetens ledelse. Dette påvirker sikkerhetskulturen i virksomhetene og avgjør hvor stort fokus og prioritet sikkerhets- og beredskapsarbeidet får • Hvordan virksomhetene jobber med beredskap og inkluderer digital sikkerhet i dette varierer • Kunnskap og kompetanse når det kommer til datakriminalitet spiller inn på virksomhetens risikoforståelse, og er sentralt i hvordan virksomhetene forholder seg til trusselen som datakriminalitet utgjør • En helhetlig tilnærming til sikkerhet forankret i et godt beredskapsplanverk vil kunne øke virksomhetens modenhet og med det forståelsen for viktigheten av åpenhet og informasjonsdeling med politiet
Hvilke faktorer spiller inn på virksomhetenes beslutning om å kontakte politiet dersom de blir utsatt for datakriminalitet?	• Til tross for at mange virksomheter har forankret kontakt med politiet i forbindelse med datakriminalitet i sine beredskapsplaner tas det ofte situasjonsbestemte vurderinger rundt å involvere politiet • Virksomhetens vurderinger rundt kost/nytte, egeninteresse og tid og prioriteringer står sentralt. Dette baserer seg på hva virksomhetene vurderer at de vil få ut av et samarbeid med politiet • Omdømme er viktig for virksomhetene. Virksomhetene fokuserer på de positive effektene det vil kunne ha for virksomhetens omdømme når det kommer til å dele informasjon med politiet om datakriminalitet og involvere politiet dersom virksomheten har blitt utsatt for datakriminalitet
Hvilke forventninger har virksomhetene til politiet når det kommer til samarbeid og forebygging og håndtering av datakriminalitet?	• Flere av virksomhetene vet ikke hva som er realistiske forventninger å ha til norsk politi når det kommer til datakriminalitet, derfor snakker de om ønsker i tillegg til forventninger. Dette baserer seg på opplevelsen av at politiet har kommet sent på banen og at datakriminalitet ikke har blitt prioritert • Virksomhetene forventer at politiet evner å samarbeide internasjonalt, at politiet fortsetter satsningen på næringslivskontakter og at det etableres gode rutiner og systemer for å ta imot og forvalte den informasjonen virksomhetene deler med politiet om datakriminalitet • Virksomhetene ønsker at politiet i større grad skal dele informasjon, kunnskap og erfaringer med virksomhetene som de kan benytte i sitt beredskapsarbeid og som kan bidra til at virksomhetene blir satt i bedre stand til å beskytte seg mot datakriminalitet • Virksomhetene ønsker tydeligere kommunikasjon fra politiet om hva politiet ønsker fra virksomhetene og hvordan virksomhetene skal forholde seg til mindre alvorlig og alvorlig datakriminalitet • Virksomhetene forventer ikke nødvendigvis at politiet skal kunne hjelpe dem med en situasjon dersom de har blitt utsatt for alvorlig datakriminalitet, men de forventer rask respons og et politi som kan bistå med råd, veiledning og beslutningsstøtte

	• Virksomhetene opplever at det kun er et spørsmål om tid før de opplever å bli utsatt for alvorlig datakriminalitet. Dette er i seg selv et godt argument for å prioritere beredskapsarbeid og etablere et godt samarbeid med politiet.
Hva kan politiet gjøre for å legge bedre til rette for et godt samarbeid med virksomhetene?	• Øke kapasitet og kompetanse, samt prioritering av datakriminalitet gjennomgående i politiet • Etablere trygge og nøytrale arenaer for deling av informasjon, kunnskap og erfaringer mellom virksomhetene og politiet. For eksempel seminarer • Senke terskelen for kontakt gjennom næringslivskontakter • Bidra med informasjon til virksomhetene om tusler og trender knyttet til datakriminalitet i før-, under- og etterkrisefasen
Hvordan spiller samfunnet, media og datakriminalitetens natur inn på samarbeidet mellom politiet og virksomhetene?	• Medias fremstilling av virksomheter som har blitt utsatt for alvorlig datakriminalitet kan påvirke valg om åpenhet, og det kan påvirke hvorvidt virksomhetene deler informasjon og involverer politiet. Dette henger sammen med virksomhetenes omdømme og samfunnets forståelse av trusselen datakriminalitet utgjør • Virksomhetenes komplekse målgruppe gjør at virksomhetene har et behov for kontroll når det kommer til å styre hvilken informasjon som kommer ut dersom de blir utsatt for datakriminalitet. Godt samarbeid med politiet for å koordinere kommunikasjon utad er sentralt i dette • Holdninger og antakelser hos virksomhetene om at det å kontakte politiet er ensbetydende med at informasjonen blir offentlig kjent kan påvirke om virksomhetene kontakter politiet • Det er krevende for virksomhetene å ha en oppdatert og god risikoforståelse når det kommer til datakriminalitet grunnet et hurtig skiftende trusselbilde

Tabell 4.2 Kobling mellom forskningsspørsmål og empiriske funn.

5 Analyse

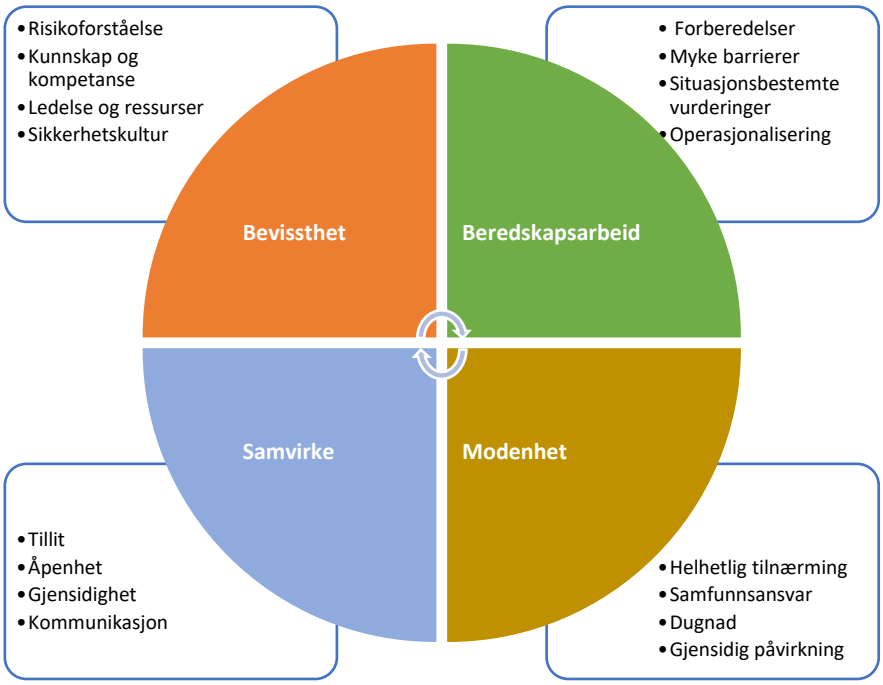
Problemstillingen for denne studien er: «*Hvilke faktorer påvirker norske virksomheters samarbeid med politiet når det kommer til forebygging og håndtering av datakriminalitet?*».

Gjennom problemstillingen og de tilknyttede forskningsspørsmålene, har jeg fått et omfattende datagrunnlag gjennom datainnsamlingen. De viktigste funnene i studien dreier seg om menneskelige og organisatoriske faktorer i de norske virksomhetene og politiet som påvirker samarbeidet når det kommer til forebygging og håndtering av datakriminalitet. Dette er faktorer som risikoforståelse, kunnskap og kompetanse, sikkerhetskultur, allokering av tid og ressurser til sikkerhets- og beredskapsarbeidet, ledelsens involvering og opptatthet av sikkerhet, helhetlig tilnærming til sikkerhet og viktigheten av gode forberedelser gjennom beredskapsarbeidet. I dette ligger også faktorer som kommunikasjon og prinsipper for samarbeid, åpenhet og elementer knyttet til politiets arbeid med datakriminalitet. Dette er også faktorer som går igjen i teorien. De empiriske funnene og kjerneelementene fra det teoretiske rammeverket ledet med det til de mest sentrale funnene i oppgaven som utgjør de fire områdene:

- Bevissthet – Risikoforståelse, ledelse og digital sikkerhetskultur
- Beredskapsarbeid – Viktigheten av gode forberedelser
- Samvirke – Tillit, åpenhet og gjensidighet
- Modenhet – Samspillet mellom virksomhetenes og politiets arbeid med datakriminalitet

Figur 5.1 er en overordnet og forenklet modell som viser de fire områdene. Det er innenfor disse fire områdene hovedvekten av funn ligger med utgangspunkt i den informasjonen informantene kom med, i tillegg til at disse momentene er sentrale i det teoretiske rammeverket. Modellen viser knytningen mellom de mest sentrale funnene og elementer som kom frem gjennom datainnsamlingen, samt hvordan de mest sentrale funnene spiller inn på hverandre.

Forebygging og håndtering av datakriminalitet – faktorer som påvirker samarbeidet



Figur 5.1 En overordnet modell som viser fire områder som inneholder faktorer som påvirker samarbeidet mellom de norske virksomhetene og politiet

De fire områdene vil bli videreført i analysen og drøftet i dette kapitlet. Teorien som ble presentert i kapittel 2 danner grunnlaget for analysen, sammen med nyere og internasjonal forskning innen tematikken. Jeg vil videre ta for meg de fire områdene, og drøfte og analysere disse inngående opp mot det teoretiske rammeverket. De fire områdene inneholder informasjon fra empirien som kom frem gjennom hovedkategoriene «Politiet og datakriminalitet», «Virksomhetenes beredskapsarbeid» og «Datakriminalitet, media og samfunnet». I analysen har jeg valgt å innlemme disse hovedkategoriene i de fire områdene siden med bakgrunn i at liknende informasjon kommer frem under de forskjellige hovedkategoriene og henger sammen og påvirker hverandre. Disse sammenhengene blir behandlet i de fire områdene noe som var mer hensiktsmessig, heller enn hver for seg. På denne måten blir det også mer dybde i analysen.

5.1 Bevissthet

Flere av beredskapsteoriene har et fokus på bevissthet i en eller annen form, og gjennom empirien kom det frem at bevissthet både kan knytte seg til forståelse, kunnskap, kompetanse og informasjonsbehandling. I denne sammenheng knyttes bevissthet til risiko, og det handler om det at individer og virksomheten som et kollektiv er bevisst trusler, sårbarheter og verdier.

5.1.1 Risikoforståelse - kunnskap og bevisstgjøring

Hvordan virksomheter forholder seg til risiko baserer seg på hvordan risikoen blir forstått individuelt og av virksomheten som et kollektiv. Risikoforståelse varierer og avhenger av forskjellige forhold som tilgang til informasjon, kompetanse, kontekst, kunnskap om trusler, verdier og sårbarheter. Risikoforståelse blir med det subjektivt fordi vi vil oppleve risiko forskjellig (Turner, 1978, Aven et al., 2019, s. 37-41;). Kompetanse, læring og risikoforståelse er knyttet til hverandre, og god risikoforståelse er en avgjørende faktor i sikkerhetsarbeidet (Reason, 1997, s. 7; Aven et al., 2019; Bergsjø et al., 2020, s. 39) Dersom virksomheten ikke har kunnskap om truslene fra datakriminelle, teknisk forståelse og innsikt kan det være vanskelig å vite hvilke trusler man står overfor og hvilke sårbarheter som eksponeres. Datakriminalitet kan oppleves «mindre synlig» og håndgripelig enn kriminalitet ellers, noe som kan skape utfordringer når det kommer til forståelsen av risiko (Nätt & Heine, 2019; Aakre, 2020, s. 19).

I mørketallsundersøkelsen (2020) kommer det frem at blant de norske virksomhetene som deltok i undersøkelsen og som har opplevd datakriminalitet, mente 64% av virksomhetene at de største årsakene til at hendelsen skjedde var som følge av tilfeldigheter eller uflaks, mens halvparten mente at sikkerhetsbruddet oppstod på grunn av menneskelige feil. Videre kommer det frem at det var like mange av virksomhetene som svarte at datakriminaliteten ble oppdaget ved en tilfeldighet som ved rutinemessig intern sikkerhetsmonitorering (NSR, 2020). At tilfeldigheter og uflaks trekkes frem som årsaker til at datakriminalitet oppstår og at mange uønskede hendelser blir oppdaget ved tilfeldigheter, kan knyttes manglende risikoforståelse og kunnskap i norske virksomheter når det kommer til datakriminalitet.

Turner (1978) mente at en av utfordringene organisasjoner kan møte på når det kommer til risikoforståelse og sikkerhetsarbeid er for store mengder informasjon å forholde seg til eller ignorering av eksisterende informasjon. I dag eksponeres vi for store mengder informasjon og for å etablere risikoforståelse må vi velge ut deler av informasjonen som er relevant for oss.

Derfor vil forståelse for og kunnskap om de truslene vi er utsatt for være sentralt når det kommer til risikoforståelse (Renn, 2008, s. 99). Informantene fra utvalg 1 opplever datakriminalitet og truslene fra det digitale rom som et krevende felt. Dette har bakgrunn i det hurtig skiftende trusselbildet, at datakriminaliteten gjerne er grenseoverskridende og kompleks, at denne formen for kriminalitet ikke «synes» på samme måte som kriminalitet som foregår i det fysiske rom, i tillegg til at de datakriminelle har blitt så profesjonelle og kreative at virksomhetene kan føle på en form for håpløshet når det kommer til å beskytte seg. Informantene forteller også om en opplevelse av at det kun er et tidsspørsmål før deres virksomhet blir utsatt for alvorlig datakriminalitet for første gang eller igjen. De forteller alle om store mengder forsøk på mindre alvorlig datakriminalitet gjennom for eksempel phishing e-poster. Flere informanter i utvalg 2 nevner at datakriminalitet ofte får mindre oppmerksomhet av samfunnet enn andre former for kriminalitet, noe som kan forklares med at mange synes datakriminalitet er vanskelig å forholde seg til fordi man ikke har kunnskap nok eller opplever den som mer abstrakt og mindre håndgripelig. Datakriminalitet som en «mindre synlig» form for kriminalitet i kombinasjon med et hurtig skiftende trusselbilde med mye informasjon kan gjøre det vanskelig for virksomhetene å etablere en god risikoforståelse. Dette kan påvirke samarbeidet med politiet gjennom at virksomhetene ikke helt vet hva de blir utsatt for og at kriminaliteten ikke nødvendigvis blir oppdaget dersom den ikke er «alvorlig nok». Kompetanseheving og kunnskap vil i denne sammenheng kunne være viktig for at virksomhetene i større grad kan øke sin bevissthet og risikoforståelse og med dette i større grad evne avdekke og rapportere hendelser til politiet.

I virksomheter vil det kunne oppstå et «informasjonsgap» mellom de kollektive antakelsene om risiko som baserer seg på kulturen i virksomheten og kunnskapen om det som faktisk truer virksomheten. Risikostyring kan være utfordrende, nettopp fordi risiko oppfattes ulikt. Det er ikke uvanlig at man i etterkant av uønskede hendelser avdekker et mangelfullt kunnskapsgrunnlag og begrensninger i virksomhetens kollektive risikoforståelse og evne til å forebygge og håndtere uønskede hendelser (Turner, 1978). Flere av informantene i utvalg 1 forteller om hvordan fokuset på risikoforståelse og kompetanse innen digital sikkerhet har fått økt oppmerksomhet de siste årene. Kompetansen bygges gjerne gjennom å være en del av bransjenettverk som deler erfaring og informasjon, gjennom å få bistand fra eksterne sikkerhetsselskaper, ansettelse av personer med kompetanse og ved å delta på kurs og utdanning. I tillegg er det et fokus på å lære av hendelser som har truffet andre virksomheter som de kan sammenligne seg med, og dra nytte av andres erfaringer. Selv om informantene

fra utvalg 1 aktivt søker informasjon og kunnskap om truslene fra de datakriminelle, ønsker de i større grad informasjon fra politiet som kan hjelpe dem med å etablere en bedre risikoforståelse. Flere har opplevelser med at private sikkerhetsselskaper deler informasjon med en «skjult agenda», som for eksempel å selge sikkerhetsløsninger. Virksomhetene investerer i løsninger for datasikkerhet med et ønske om å minimere risikoen. Investeringene i sikkerhetsløsninger baserer seg gjerne på virksomhetenes frykt, og ikke nødvendigvis kunnskap og god risikoforståelse (Bergsjø et al., 2020, s. 204). Informantene i utvalg 1 forteller at dersom politiet i større grad hadde bidratt med denne informasjonen kunne virksomhetene basert risikoforståelsen sin på informasjon fra en nøytral og pålitelig kilde. De nevner også at informasjon fra politiet gjerne tillegges stor verdi i virksomhetens ledelse og sikkerhetsavdelinger. Informantene tilknyttet politi- og lensmannsetaten uttalte at det er et sentralt element i politiets forebyggende strategi når det kommer til datakriminalitet å sette virksomhetene i bedre stand til å beskytte seg selv, blant annet gjennom å kunne dele informasjon om trusselbildet (POD, 2020).

Hva som anses for å være «riktig kunnskap» knyttes gjerne til ekspertise, og det finnes mange aktører å lytte til når det kommer til datakriminalitet og digital sikkerhet (Bergsjø et al., 2020, s. 40). I teorien om høypålitelige organisasjoner er ett av de fem prinsippene for å oppnå høy pålitelighet anerkjennelse av kompetanse. Dette handler i utgangspunktet om å utnytte virksomhetens interne kompetanse på best mulig måte. Samtidig handler det også om å identifisere og erkjenne manglende kunnskap slik at man tilegne seg denne kompetansen, for eksempel gjennom hjelp fra ekstern ekspertise (Weick & Sutcliffe, 2015). Ifølge samvirkeprinsippet har virksomhetene et selvstendig ansvar for å sikre best mulig samarbeid med relevante aktører i arbeidet med forebygging, beredskap og krisehåndtering (Engen et al., 2021, s. 325). Sett i sammenheng med virksomhetenes ønske om at politiet i større grad skal være en ledende kilde til informasjon om datakriminalitet vil dette kunne gjøre det enklere for virksomhetene å etablere et godt risikobilde da de i større grad kan forholde seg til en pålitelig, troverdig og nøytral kilde til informasjon. Samtidig som politiet ville kunne bidratt til at virksomhetene kunne etablere god risikoforståelse, er det likevel viktig at politiet ikke blir den eneste kilden til informasjon om datakriminalitet da politiet ikke vil ha anledning til å vite alt. Samarbeidet mellom flere offentlige og private aktører vil bidra til et mer helhetlig bilde, og virksomhetene må forholde seg til informasjon utover det politiet kommer med, noe som er i tråd med den nasjonale strategien for digital sikkerhet (Departementene, 2019).

Datasikkerhet kan ses på som en bevissthet om hva datakriminelle kan gjøre og hvordan man kan hindre at ondsinnede handlinger skjer. Det kan også være bevissthet om hvordan man oppdager at noe har skjedd og hvordan man kan begrense skadene, det er altså både kunnskap og en måte å tenke på (Nätt &Heide, 2019, s. 17). Dersom den kollektive risikoforståelsen i en virksomhet ikke gjenspeiler de faktiske truslene virksomheter i dag står overfor, kan dette påvirke hvordan virksomheten forholder seg til trusler, sårbarheter og verdier, og hvordan de jobber med digital sikkerhet og samarbeider med andre aktører. Dersom politiet i større grad hadde bidratt med informasjon til virksomhetene kan det tenkes at informasjonen politiet hadde fått fra virksomhetene kunne ha kommet tidligere og holdt høyere kvalitet, noe som igjen kunne ha bidratt til at politiets forebyggende arbeid hadde blitt mer effektivt og kunne basert seg på et oppdatert kunnskapsgrunnlag (POD, 2020). Et annet moment som kunne ha bidratt til et bedre samarbeid mellom norske virksomheter og politiet er større bevissthet hos virksomhetene når det kommer til hvordan politiet jobber med datakriminalitet. Flere av informantene i utvalg 1 forteller at de ikke alltid assosierer datasikkerhetshendelser, eller datakriminalitet, med politiet, noe som kan komme av hvilken forståelse de har av hva datakriminalitet er og hva politiet viser at de jobber med. Flere av informantene ga også uttrykk for at virksomhetene har manglende kunnskap om hvordan politiet jobber med datakriminalitet og hva politiet kan bidra med både når det kommer til forebygging og håndtering. Dette viser hvordan kommunikasjon mellom politiet og virksomhetene også er en viktig faktor som kan påvirker samarbeidet.

Samtidig som virksomhetene ønsker informasjon om datakriminalitet fra politiet, er politiet avhengig av informasjon fra virksomhetene om hva som foregår, hvilke utfordringer de står i og hvilke trusler og hendelser de er utsatt for. Dette fremstår som et dilemma for «begge parter» i samarbeidet mot datakriminaliteten. Politiets informasjonsdeling knyttes tett til kompetanse og kapasitet når det kommer til datakriminalitet, og politiet jobber mot å i større grad kunne dele relevant og tidsriktig informasjon med virksomhetene. Samtidig har politiets kompetanse og kapasitet vist seg å være mangelfull, noe som gjør det vanskelig for politiet å bidra tilstrekkelig med informasjon til virksomhetene da arbeidet med datakriminaliteten tar tid å etablere. Dette har også ført til at andre aktører, offentlige og private, har kommet på banen, og virksomhetenes risikoforståelse baserer seg med det på informasjon om datakriminalitet fra mange forskjellige aktører som ikke har det samme mandatet som politiet (Riksrevisjonen, 2021). Det er tydelig ønske i norske virksomheter og hos politiet om å få til et bedre samarbeid basert på utveksling av informasjon begge veier og

deling av erfaring. Kombinasjonen av risikoforståelse og kunnskap om datakriminalitet samt bevissthet rundt hvordan politiet jobber vil kunne bidra positivt inn i et samarbeid mellom de norske virksomhetene og politiet.

5.1.2 Forankring i ledelsen og sikkerhetskultur

Mangelfull planlegging, styring og gjennomføring av det digitale sikkerhetsarbeid i norske virksomheter har flere ganger vært et tema i NSM sine årlige risikovurderinger, noe som kan knyttes til en manglende risikoforståelse hos ledelsen i virksomhetene (NSM, 2017; Bergsjø & Windvik, 2018). Ifølge Turner (1978) er sikkerhetskulturen og den kollektive risikoforståelsen i en virksomhet sentrale elementer når man skal se på bakgrunnen for at ulykker skjer, fordi mangelfull sikkerhetskultur og feil risikoforståelse kan lede til alvorlige uønskede hendelser. Flere av informantene i utvalg 1 forteller om en utvikling hos ledelsen når det kommer til risikoforståelse knyttet til datakriminalitet. Tidligere ble det digitale sikkerhetsarbeidet ofte tillagt IT-avdelingen, og dermed atskilt fra resten av virksomheten. Manglende kunnskap og forståelse hos ledelsen gjorde at ikke det digitale sikkerhetsarbeidet ble prioritert høyt nok i virksomhetens helhetlige sikkerhetsarbeid, og det fikk heller ikke det fokuset og prioriteringen som var nødvendig.

Sikkerheten i en virksomhet avhenger av at sikkerhetsarbeidet forankres i ledelsen. Det er ledelsen som har ansvaret for sikkerheten, selv om det gjerne er utpekte personer som jobber mer direkte med dette. I tillegg til et ansvar for sikkerheten har ledelsen et ansvar for den digitale sikkerhetskulturen. Det bør settes klare mål for sikkerhetsarbeidet som ledelsen kan følge opp, og det må avsettes ressurser til arbeidet slik at virksomhetene kan jobbe målrettet med sikkerhet over tid på en helhetlig måte (Bergsjø & Windvik, 2018, s. 13; Bergsjø et al., 2020, s. 43 og 120). Kompetanseheving og økt risikoforståelse hos ledelsen når det kommer til datakriminalitet og truslene fra det digitale rom trekkes frem i begge utvalgene som en viktig faktor i arbeidet med sikkerhet i virksomhetene. Flere av informantene i begge utvalg nevnte at det er viktig at politiet retter informasjon og kunnskapsheving mot virksomhetenes ledelse for å etablere en risikoforståelse som genererer fokus og prioritering av sikkerhetsarbeidet. I denne sammenheng forteller flere av informantene i utvalg 1 om viktigheten av å få informasjon fra «ekspertene», her politiet, for å etablere en god risikoforståelse hos ledelsen. Informasjon fra politiet blir ofte tillagt stor verdi hos virksomhetens ledere. I utvalg 2 er det også flere av informantene som trekker inn ledelsen som et viktig element når det kommer samarbeidet med politiet fordi ledelsen ofte vil være

sentral i beslutningen om hvorvidt informasjon om datakriminalitet skal deles med politiet, eller ikke, hvordan en hendelse skal håndteres og hvor mye ressurser, tid og fokus sikkerhetsarbeidet i virksomheten skal få. Dette mener flere av informantene i utvalg 2 at har en direkte innvirkning på samarbeidet mellom virksomhetene og politiet, fordi det til syvende og sist er ledelsen som bestemmer hvordan virksomheten skal forholde seg til datakriminalitet.

Flere kjente beredskapsteorier fokuserer på viktigheten av ledelsens forpliktelse til arbeidet med sikkerhet, og hvordan deres holdninger og fokus på sikkerhet kan spille inn på sikkerhetskulturen i virksomheten (Reason, 1997; Weick & Sutcliffe, 2015; Turner, 1978). Turner (1978) mente at virksomhetens sikkerhetskultur reflekterer ledelsens prioritering og fokus på sikkerhet. Informantene i utvalg 1 forteller at når ledelsen går foran i jobben med digital sikkerhet er det enklere å få med hele virksomheten og dra lasset sammen mot en bedre digital sikkerhetskultur. Noen av informantene forteller også om ledere som har virkelig har forstått hvilken trussel datakriminalitet og annen aktivitet på den digitale arena utgjør, noe som har gjort at sikkerhetsarbeidet får høy prioritet.

Selv om informantene fra utvalg 1 maler et bilde av en økt risikoforståelse og bevissthet hos ledelsen når det kommer til datakriminalitet og truslene fra det digitale rom, vil prioriteringen av sikkerhet alltid konkurrere mot produksjon når det kommer til allokering av ressurser. I Reason sin teori om organisatoriske ulykker (1997) er latente forhold i en organisasjon sentrale når det kommer til å forklare årsaken til ulykker. Teorien fokuserer på organisatoriske forhold heller enn menneskelige feil. De organisatoriske forholdene baserer seg gjerne på beslutninger fattet av virksomhetens ledere. Sett i sammenheng med risikoforståelse, kunnskap og bevissthet rundt truslene fra datakriminelle vil det være sentralt at ledere i virksomheter allokerer ressurser til arbeidet med beredskap og digital sikkerhet. I en ideell verden bør sikkerheten i en virksomhet gjenspeile de truslene som virksomhetens produksjon er utsatt for. Informasjon relatert til produksjon er gjerne direkte og konkret, kontinuerlig og gjerne lett å forstå. Til sammenligning er gjerne suksessfull sikkerhet knyttet til fraværet av negative hendelser, og det er gjerne bare etter en nestenulykke eller en uønsket hendelse at sikkerhet havner øverst på ledelsens agenda. Perioder uten at man blir utsatt for alvorlige uønskede hendelser kan lede til at fokus og prioritering av sikkerhet blir nedprioritert. Man kan ende opp i en situasjon hvor man «glemmer» at det eksisterer trusler (Reason, 1997, s. 4). Begge intervjuutvalgene forteller om hvordan politiets deling av informasjon om trusler knyttet til datakriminalitet kan bidra til et mer jevnt fokus på sikkerhet.

Denne informasjonen vil kunne gjøre at ledelsen i virksomhetene kan basere sine prioriteringer av sikkerhet på et oppdatert trusselbilde, og et samarbeid med politiet vil her være sentralt for ledelsens risikoforståelse.

Flere av informantene i utvalg 1 forteller at de har en opplevelse av at det kun er et spørsmål om tid før deres virksomhet blir utsatt for alvorlig datakriminalitet. I et hurtig skiftende trusselbilde i stadig utvikling er det viktig at sikkerhetsarbeidet foregår kontinuerlig. I teorien om høypålitelige organisasjoner fremheves det å være mentalt forberedt er å forvente at noe uønsket kommer til å skje. Kjernen i denne teorien er kombinasjonen av mindfull organizing og sensemaking. Prosessen omtales som konstant meningsskapende, og baserer seg på kontinuerlig persepsjon, erfaring og forventninger (Weick & Sutcliffe, 2015, s. 35). Gjennom en slik tilnærming vil en virksomhet kunne basere sitt sikkerhetsarbeid på en kontinuerlig oppdatert risikoforståelse og utvikle sikkerhetsarbeidet i takt med trusselutviklingen. Ifølge informantene i utvalg 1 virker de fleste lederne i informantenes virksomheter å være positive til et samarbeid med politiet, samtidig som fokuset på og midlene til sikkerhetsarbeid varierer. Ruben i politi- og lensmannsetaten nevner at når viktig informasjon tilhørende en virksomhet først har kommet på avveie så får man sjeldent gjort noe med det. God risikoforståelse hos ledelsen vil kunne gjøre at sikkerhetsarbeidet kan forhindre at alvorlig datakriminalitet får katastrofale konsekvenser for virksomheten, og kontinuerlig jobbing med sikkerhet vil kunne sette virksomheten i bedre stand til å samarbeide med politiet og dra nytte av de erfaringene og den informasjonen politiet besitter.

De organisatoriske forholdene baserer seg gjerne på beslutninger fattet av ledere. Dette trenger ikke å være dårlige beslutninger, sett i lyset av den konteksten de er fattet i, men de kan over tid skape latente forhold i organisasjonen. Et eksempel på dette kan være at det allokeres mer penger i budsjettet til enkelte områder av de organisatoriske aktivitetene enn andre, noe som kan skape utilsiktede svakheter (Reasjon, 1997, s. 11). Ofte vil valg av sikkerhetstiltak bli avveid mot økonomiske og tidsmessige hensyn, og organisasjonens sikkerhetskultur vil kunne virke avgjørende for om en velger snarveier og lettvinte løsninger på bekostning av målene for sikkerhet (Aven et al., 2019, s. 34). Flere av informantene i utvalg 1 forteller om utfordringer knyttet til å skulle lede arbeidet med sikkerhet i en virksomhet. Utfordringene var blant annet knyttet til å kommunisere informasjon om trusler knyttet til datakriminalitet til ledelsen og at dette førte til at ledelsen prioriterte nok tid og penger til sikkerhetsarbeidet. God digital sikkerhet vil koste en del på kort sikt dersom man må gjøre store investeringer i for eksempel teknologiske løsninger. Dette vil avta ettersom

virksomheten får den digitale sikkerheten på plass. I tillegg til å bruke penger på sikkerhetsløsninger er det svært viktig at virksomheten fokuserer på kompetanse og utvikler en god digital sikkerhetskultur i virksomheten (Bergsjø & Windvik, 2018, s. 197). Begge intervjuutvalgene trekker frem at det er mye en virksomhet kan gjøre utover det å bruke penger på sikkerhetsløsninger, som for eksempel å trene på god organisering og jobbe for en god digital sikkerhetskultur. Informantene i utvalg 1 trekker frem at virksomhetene kan ha mye å lære når det kommer til krisehåndtering og organisering av politiet som har mye kompetanse på dette området. Flere av informantene i utvalg 2 påpeker også at sikkerhet ikke alltid trenger å koste penger og at det er mye en virksomhet kan gjøre når det kommer til sikkerhetsarbeid som dreier seg om planlegging og organisering.

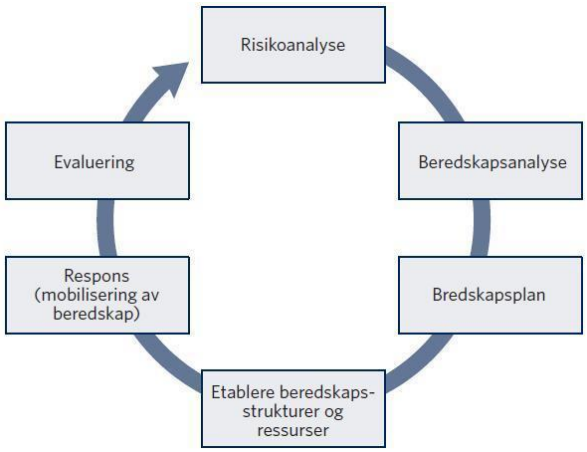
Reason (1997) har et systemisk perspektiv på årsaken til organisatoriske ulykker. Selv om vi ikke kan nekte for at menneskelige vurderinger, beslutninger og handlinger er involvert i organisatoriske ulykker, mener Reason at menneskelige feil i all hovedsak ikke skyldes individet selv, men er et resultat av forhold ved organisasjonen. I dette perspektivet ses menneskelige feilhandlinger på som en konsekvens heller enn årsak. Ifølge Reason er det viktig at man tar høyde for dette og etablerer flere lag av sikkerhet slik at aktive feil begått av mennesker fanges opp og ikke får bli den eneste kilden til feil som kan få alvorlige konsekvenser. Reason mente at man ikke kan forandre den menneskelige faktoren, men man kan forandre forholdene mennesker jobber under (Reason, 1997, s. 15). I utvalg 1 kommer det frem at ledelsen har stor påvirkning når det kommer til hvordan virksomheten jobber med digital sikkerhet. Dette handler både om hvor mye fokus, tid og ressurser det digitale beredskapsarbeidet får, men også hvordan de som jobber med sikkerhet blir sett på dersom det går galt. Flere av informantene følte at de kunne havne mellom barken og veden ved at de ble ansett som kompetente når det ikke skjer noe uønsket i virksomheten, men at de kan få skylden dersom virksomheten blir rammet av alvorlig datakriminalitet. I denne forbindelse trekker flere av informantene frem viktigheten av et tett samarbeid med politiet både når det kommer til informasjonsdeling og risikoforståelse, men også for å kunne få mer tyngde gjennom informasjon fra politiet når de argumenterer for sikkerhet til ledelsen. Informantene ønsket også en tettere kontakt med politiet for å kunne få bistand, råd og veiledning dersom virksomheten ble utsatt for alvorlig datakriminalitet.

5.2 Beredskapsarbeid – viktigheten av gode forberedelser

Som nevnt er beredskap og forebygging sentralt i arbeidet med samfunnssikkerhet. Formålet med beredskap er å forutse mulige trusler og utfordringer slik at de kan håndteres på en effektiv måte. Beredskap kan også ses på som en prosess, et produkt, en aktivitet og en tilstand (Engen et al., 2021, s. 321). Informanter fra begge utvalgene trakk frem at virksomhetenes beredskapsarbeid er sentralt når det kommer til samarbeid med politiet. Dette handler både om hvordan virksomhetene forholder seg til mindre alvorlig datakriminalitet i det daglige, og hvordan de forholder seg til politiet dersom de blir utsatt for mer alvorlig datakriminalitet som for eksempel et dataangrep med løsepengekrav. De viktigste momentene når det kommer til dette er hvorvidt virksomhetene og ledelsen har tatt stilling til hvordan de forholder seg til datakriminalitet og samarbeid med politiet i forkant av at en alvorlig hendelse skjer, og i det daglige når de blir utsatt for mindre alvorlig datakriminalitet.

5.2.1 Beredskapsarbeidets faser og operasjonalisering av tiltak

Beredskapsarbeidet gjennomføres i all hovedsak i førkrisefasen. I den akutte krisefasen skjer selve mobiliseringen av beredskapen. I etterkrisefasen handler det om å komme tilbake til normaltilstand og evaluere håndteringen og lære av feilene (Engen et al., 2021, s. 328).



Figur 5.2 *Faser i beredskapsarbeid.* Fra *Perspektiver på samfunnssikkerhet* (s.325), av Engen et al., 2021. Cappelen Damm Akademisk

Beredskapsarbeidet kan deles inn i ulike faser. Arbeidet er syklisk og bør skje kontinuerlig, men også i en viss rekkefølge hvor fasene bygger på hverandre. Det er grunnleggende at man starter med å gjennomføre en risikoanalyse for å etablere kunnskap om trusselen og for å kartlegge og beskrive risikoen. Risikoanalysen er en systematisk prosess og

man tar gjerne utgangspunkt i identifiserte farer og trusler, for så å gjennomføre årsaks- og konsekvensanalyser av disse. Risikoanalysen bidrar til bedre risikoforståelse (Engen et al., 2021, s. 325). Ruben, fra politi- og lensmannsetaten, trekker frem at han har opplevd at mange virksomheter ikke har et bevisst forhold til hvilke konsekvenser alvorlig datakriminalitet kan ha for dem.

> Du kan rette opp mye, men du får ikke rettet opp i informasjon på avveie til fri benyttelse for kriminelle. Og det er veldig få virksomheter som har tatt innover seg hva som skjer dersom de mister sine innerste bedriftshemmeligheter. Det er en sånn «tilleggs-dimensjon» som jeg ser at det er veldig få som har et bevisst forhold til. Det er ikke så mange som gjennomfører skikkelige konsekvensanalyser (Ruben, Politi- og lensmannsetaten).

Fra risikoanalysen tar man med seg er identifiserte trusler for å etablere en oversikt over utvalgte uønskede hendelser man skal bygge beredskap for å håndtere. Sondre, fra et privat sikkerhetsselskap, påpeker at man gjennom denne fasen kan få en oversikt over egne verdier og sårbarheter, noe som er viktig for å vurdere truslene. Videre følger en beredskapsanalyse som har til hensikt å identifisere virksomhetens ambisjoner for sin beredskap samt beredskapsressursene som virksomheten skal sette av for å kunne respondere uønskede hendelser. Risiko- og beredskapsanalysen skal resultere i en oversikt over aktuelle farer vi skal forberede oss på å håndtere, og si noe om dimensjoneringen av beredskapen for dem, de skal altså si noe om ressursbehovene (Engen et al., 2021, s. 326). Beredskapsanalysen vil kunne vise hvilke ressurser virksomheten selv har og kan benytte seg av under en krise. I teorien om høypålitelige organisasjoner er anerkjennelse av kompetanse et viktig prinsipp som går ut på å utnytte den kompetansen organisasjonen har internt på best mulig måte i en krise. I denne sammenheng må man se på hvordan virksomheten skal organisere seg da det kan bli et behov for å desentralisere beslutningsmyndighet slik at de mest kompetente personene sitter sentralt i beslutningsprosessen. I tillegg handler det i dette prinsippet om å identifisere manglende ressurser og kompetanse og se hvor man kan skaffe dette (Weick & Sutcliffe, 2015). Her vil det være sentralt for virksomhetene å se på hvilke ressurser som skal benyttes ved en krise og etablere kommunikasjonslinjer til ekstern kompetanse. Dette er også i tråd med samvirkeprinsippet (Engen et al., 2021, s. 325), og virksomhetene bør her vurdere hvordan de skal forholde seg til politiet og vite hva politiet kan bidra med.

Risiko- og beredskapsanalysen danner grunnlaget for beredskapsplanen som skal beskrive hvem som har ansvar for hva, hvor, når og hvordan beslutninger skal fattes. Den

beskriver hvilken beredskap man trenger for å for å håndtere truslene virksomheten står overfor og beskriver hva slags beredskapsstrukturer som skal etableres og hvilke ressurser som skal allokeres. Beredskapsplanen skal sikre at responsen i en krise er planlagt, forutsigbar, effektiv og koordinert. Mobilisering av beredskapen kan utføres i forbindelse med reelle hendelser eller trening og øving (Engen et al., 2021, s. 326). Kristoffer fra politi og lensmannsetaten forteller om viktigheten av å operasjonalisere beredskapsplanverket, altså å teste planene for å se at de faktisk fungerer og eventuelt gjøre endringer. Han forteller at det er stor forskjell i hvordan virksomhetene forholder seg til dette.

> I dag har nok mange virksomheter tatt høyde for dataangrep i risiko- og sårbarhetsanalysene sine. I noen sektorer er man i større grad pålagt å utføre en beredskapsanalyse, men så er det mange virksomheter som ikke har en beredskapsanalyse i det hele tatt. Veldig mange har kanskje gjennomført det sånn at det ser bra ut på papiret og tenker nok også litt sånn «check» da har vi tatt høyde for det. Men for å gjør dette riktig så skal man analysere risiko og sårbarhet, så skal man sammen med ledelsen komme med tiltak og løsninger på disse situasjonene. Man må altså operasjonalisere de tiltakene man kommer frem til og teste at det fungerer (Kristoffer, Politi- og lensmannsetaten).

Beredskapsplanlegging kan også resultere i «fantasidokumenter» som virksomhetene stoler så mye på at de ignorerer praktiske erfaringer og som kanskje bygger på ressurser som i realiteten kanskje vil være utilgjengelige (Clarke & Perrow, 1996, referert i Engen et al., 2021, s. 335). I likhet med fantasidokumenter er symbolsk beredskap en beredskap som ikke reflekterer de operative realitetene. En konsekvens av dette er at beredskapen kan danne en synergi, samarbeidsrelasjoner og forutsigbarhet som kun eksisterer i planen, og den kan ikke brukes som grunnlag for respons i kriser (Engen et al., 2021, s. 335). Flere av informantene i utvalg 2 trekker frem at virksomhetene må implementere myndighetskontakt i beredskapsplanene sine og at de bør trene på å etablere kontakt. Med dette mener de at virksomhetene gjennom beredskapsarbeidet må ta stilling til hvordan de skal forholde seg til politiet og andre relevante myndigheter, spesielt dersom de blir utsatt for alvorlig datakriminalitet. Kristoffer fra politi- og lensmannsetaten forklarer viktigheten av å involvere politiet så tidlig som mulig dersom virksomheten for eksempel bli utsatt for et dataangrep, da dette vil kunne være en suksessfaktor dersom politiet skal kunne hjelpe virksomheten i håndteringen av hendelsen. Begge intervjuutvalgene forteller hvordan en slik hendelse innledningsvis vil skape en svært kaotisk, krevende og uoversiktlig situasjon, og dersom man

ikke har tatt stilling til om man skal kontakte politiet kan dette fort bli nedprioritert. Vibeke fra Industri forteller om da hennes virksomhet ble utsatt for et dataangrep. Hun forteller om en kaotisk initialfase hvor mange arbeidsoppgaver seiler opp i håndteringen av krisen, og man har egentlig mer enn nok med å håndtere krisen internt. Hun forteller at da hennes virksomhet opplevde dette for første gang hadde de ikke kunnskap om at politiet burde kontaktes.

> Det vi gjorde veldig tidlig var at vi fikk kontakt med andre selskaper som hadde vært utsatt for det samme og søkte råd der. Og det var jo andre selskaper i andre land, og det var ingen av de som fremhevet kontakt med politiet. Så i løpet av den første dagen så var vi rett og slett ikke kommet dit at vi hadde bevissthet rundt at det å kontakte politiet var en klok ting å gjøre (Vibeke, Industri).

Standardisering og fastsatte planer kan føre til at man i en krise blir mer opptatt av å følge planen enn å tilpasse seg det som skjer i krisen. Planer som tilsynelatende dekker alt og fungerer bra kan følges helt til noe uventet skjer. Man kan gjennom å følge fastsatte planer få «skyggelapper», noe som gjør at man ikke evner å identifisere det ukjente. Man mister også gjerne evnen til improvisasjon (Engen et al., 2021, s. 256). Som beskrevet tidligere er datakriminaliteten ofte kompleks, grenseoverskridende og utvikler seg hurtig. I en situasjon hvor en virksomhet blir utsatt for alvorlig datakriminalitet kan det tenkes at krisehåndteringen kan bli vanskeliggjort av å følge en fastsatt beredskapsplan som ikke tar høyde for det ukjente og legger til rette for endringer og tilpasning. Dersom kontakt med politiet ikke står nevnt i en beredskapsplan er det nærliggende å tenke at dette kan føre til at virksomheten ikke ser at de bør kontakte politiet og at dette kan gå i glemmeboka eller skje for sent. Kåre fra Matproduksjon fortalte om da hans virksomhet ble utsatt for alvorlig datakriminalitet. Han forklarte hvordan de både hadde trent på å mobilisere og testet beredskapsplanverket, noe de hadde stor nytte av. I den reelle situasjonen måtte de likevel tilpasse krisehåndteringen da det var mye de ikke hadde forutsett. Han fortalte også hvordan kontakten med politiet både var effektiv og nyttig da dette var noe de hadde tatt høyde for og prioriterte i håndteringen.

Flere av informantene i utvalg 2 forteller om viktigheten av at virksomhetene har tatt stilling til et samarbeid med politiet før en hendelse inntreffer. Ifølge Bergsjø og Windvik (2018) mener at dersom kontakt med politiet er «nok en ting» man skal ta stilling til når man allerede står i en kaotisk situasjon kan det være vanskelig. De forteller også om viktigheten av å dele informasjon med politiet slik at politiet kan utføre sin rolle med forebygging, håndtering og etterforskning. Videre trekker de frem at det også er mulig for virksomhetene å ha en dialog med politiet uten at det må ende i en anmeldelse (Bergsjø & Windvik, 2018, s.

213). Informantene tilknyttet politi- og lensmannsetaten forklarer at det er viktig at virksomhetene har tatt stilling til dette med politikontakt. Det er ikke sånn at å kontakte politiet nødvendigvis må ende i en anmeldelse, og politiet kan bidra med både beslutningsstøtte og informasjon gjennom sine kanaler som kan bidra i virksomhetens hendelseshåndtering. I denne sammenheng er det viktig at virksomhetene har et bevisst forhold til hva politiet kan bidra med og at kontakten opprettes så tidlig som mulig. Dette avhenger av at beredskapsarbeidet har tatt høyde for kontakt med politiet, og at virksomhetene er trygge på hva det vil innebære.

Den siste fasen er å trekke lærdom av virkelige hendelser eller trening og øving. Lærdommen legger til rette for en forbedring av beredskapsplanen (Engen et al., 2021, s. 326). Noen av informantene i utvalg 1 representerer virksomheter som har opplevd at det har gått galt. De trekker frem hvordan fokuset på dette med digital beredskap fikk en større forankring i virksomheten etter at de ble utsatt for dataangrep. De forteller også hvordan de har fått en mer helhetlig tilnærming til sikkerhet hvor ikke digital sikkerhet lenger er noe som settes til IT-avdelingen og blir noe som ikke resten av virksomheten bryr seg om. I dagens samfunn er det vanlig å lære om risiko gjennom for eksempel media når andre har blitt utsatt for uønskede hendelser (Renn, 2008, s. 99). Flere av informantene i utvalg 1 forteller at fokuset på digital sikkerhet økte betraktelig etter dataangrepet som Hydro ble utsatt for i 2019. Oppdaterte risiko- og beredskapsanalyser gjennom kontinuerlig arbeid med beredskap, og lærdom vi kan trekke fra andre, vil kunne holde virksomhetens, og ledelsens, risikoforståelse oppdatert. Ofte blir ressurser til sikkerhet prioritert etter en uønsket hendelse (Reason, 1997, s. 6). Dersom man i større grad har et aktivt og oppdatert forhold til trusler og konsekvenser kan det tenkes at dette kan bidra til å opprettholde fokuset, prioriteringen og allokeringen av tid og ressurser til sikkerhet i virksomheten, noe som igjen kan øke et fokus på og effekten av et samarbeid med politiet. Flere av informantene trekker også frem politiets arbeid med Hydro-saken som noe som har fått dem til å forstå mer av hvordan politiet jobber og at det faktisk vil kunne ha stor effekt å samarbeide med politiet i forbindelse med datakriminalitet.

5.2.2 Mindful organizing, sensemaking og myke barrierer

Datakriminaliteten utvikler seg raskt og henger nøye sammen med angrep mot eller omgåelse av virksomheters sikkerhetstiltak (Engen et al., 2021, s. 250). Når det kommer til sikkerhetstiltak kan dette deles inn i mennesker, teknologi og organisasjon (NSM, 2016, referert i Bergsjø et al, 2020, s. 20-21). I oppgaven fokuserer jeg i all hovedsak på hvordan

sikkerhet i forbindelse med mennesker og organisasjon spiller inn på et samarbeid mellom norske virksomheter og politiet. Sikkerhetstiltak knyttet til mennesker og organisasjon kalles også myke barrierer. Reason (1997) viser til konseptet forsvar-i-dybden når det kommer til sikkerhets- og beredskapsarbeid. Konseptet baserer seg på myke og harde barrierer som er tiltak rettet mot de menneskelige og organisatoriske forholdene. Et mangfoldig forsvar som baserer seg på flere forskjellige lag av sikkerhet kan gjøre at virksomheter kan beskytte seg mot uønskede hendelser. De myke barrierene dreier seg blant annet om rutiner, prosedyrer, kunnskap og kompetanse, trening og øving (Reason, 1997, s. 8).

Godt beredskapsarbeid kan være avgjørende i håndteringen av alvorlige uønskede hendelser. Kvaliteten på håndteringen av en krise i den akutte fasen vil avhenge av hva som er gjort av forebygging og forberedelse i førkrisefasen, og læring i etterkrisefasen (Engen et al., 2021, s. 320). Det er ikke uvanlig at sikkerhetsstyring i virksomheter blir behandlet som en «negativ» produksjonsprosess hvor man for eksempel setter mål for at man skal miste mindre tid på uønskede hendelser. Virksomheten kan likevel ikke fjerne de uønskede hendelsene, men man kan jobbe for å unngå dem. Man må heller se på effektivt arbeid med sikkerhet som noe kontinuerlig, noe som kan gjøres ved at ledelsen jevnlig måler og forbedrer prosesser, organisering, tekniske sikkerhetssystemer, budsjettplanlegging, kommunikasjon og andre elementer som er kjente faktorer som spiller inn på sikkerheten. På denne måten blir ikke sikkerhetsarbeidet noe ekstra man må gjøre, men heller en sentral del av virksomhetens kjerneaktiviteter (Reason, 1997, s. 114). I høypålitelige organisasjoner er sikkerhetsarbeidet en dynamisk og kontinuerlig prosess som baserer seg på mindful organizing og sensemaking, altså at organiseringen skjer gjennom en kontinuerlig meningsdanning gjennom persepsjon, erfaringer og forventninger (Weick & Sutcliffe, 2015, s. 35). Virksomhetens beredskapsarbeid er sentralt når det kommer til samarbeidet med politiet. En kombinasjon av myke barrierer og økt motstandsdyktighet gjennom mindful organizing vil kunne spille inn på virksomhetens samarbeid med politiet i forbindelse med datakriminalitet. Videre vil jeg trekke frem myke barrierer fra empirien som ble trukket frem som sentrale i forbindelse med virksomhetens samarbeid med politiet og se disse i sammenheng med en virksomhetens evne til å mestre hendelser, uforutsette og forutsette.

Det er viktig med gode tekniske sikkerhetsløsninger, men det er viktig å erkjenne at tekniske løsninger alene ikke kan løse alle utfordringer i denne sammenheng. Ofte spiller den menneskelige faktoren en avgjørende rolle når noen blir utsatt for datakriminalitet. Det er derfor viktig å styrke sikkerhetskunnskapen og holdningene til sikkerhet på individnivå slik at

den generelle sikkerhetskulturen i samfunnet blir styrket. (POD, 2017, s. 6). Informantene i begge utvalg trekker frem at kunnskap og kompetanse når det kommer til datakriminalitet og truslene fra det digitale rom er viktig for å kunne forholde seg til de truslene virksomheten er utsatt for. Det varierer hvorvidt virksomhetene har klart å bygge kunnskap og kompetanse gjennom hele organisasjonen og ikke bare for de menneskene som jobber mer direkte med den digitale sikkerheten. Flere av informantene i utvalg 1 forteller at virksomheten de jobber har et fokus på å øke kompetansen og kunnskapen både hos ledelsen og de ansatte. I tillegg til kunnskap og kompetanse om datakriminalitet og trusselen fra det digitale rom er det viktig med kunnskap om politiets arbeid med datakriminalitet og hva politiets rolle og mandat er, og hva politiet kan bidra med. Det er også et ønske om at politiet skal dele mer av sin informasjon og erfaring til virksomhetene.

I teorien om høypålitelige organisasjoner er opptatthet av feil et prinsipp for å oppnå høy pålitelighet over tid. Prinsippet belyser viktigheten av en kontinuerlig oppmerksomhet rettet mot avvik og feil. Ved å ta tak i feilene kan man forhindre at situasjonen utvikler seg til noe mer alvorlig. For å kunne oppdage dette kreves det kunnskap om truslene (Weick & Sutcliffe, 2015, s. 46). Ifølge Reason (1997) faller kunnskap og kompetanse innunder kategorien myke barrierer som er rettet mot mennesker, og egner seg til å skape forståelse og bevissthet rundt trusler virksomheten står overfor. I NorSIS sine kjerneområder for digital sikkerhetskultur trekkes også kunnskap frem som et viktig element. Et eksempel på dette kan være de ansattes kunnskap om at ondsinnede vedlegg eller lenker i en e-post er en trussel mot virksomheten (NorSIS, 2018 gjengitt i Bergsjø et al, 2020, s. 40). Kunnskap og kompetanse vil kunne gjøre at ansatte i en virksomhet i større grad kan identifisere og avdekke trusler mot virksomheten som potensielt kan utvikle seg til noe mer alvorlig. For at ikke ondsinnede handlinger skal oppdages for sent og kanskje ved en tilfeldighet, må de ansatte settes i stand til å avdekke slike hendelser. Dette vil kunne bidra til at virksomheten kan ta tak i problemene før de utvikler seg til noe større og eventuelt kontakte politiet og dele informasjon om hendelsen. I tillegg kan kunnskap og kompetanse i større grad bidra til at virksomheten ikke forenkler årsaker til feil og uventede hendelser, noe som kan føre til snarveier og lettvinte løsninger i det daglige og i beredskapsarbeidet generelt. Forenklinger og generelle forklaringer på komplekse kontekster og hendelser kan vanskeliggjøre det å forestille seg uønskede konsekvenser (Weick & Sutcliffe, 2015, s. 63). Informantene i utvalg 2 påpeker at en suksessfaktor når det kommer til samarbeid med virksomhetene er en tidlig involvering, noe som kan sette politiet i stand til å for eksempel avverge at et angrep skjer mot flere andre

virksomheter. Motvillighet til å forenkle årsaker vil i større grad kunne sette virksomhetene i stand til å kontakte politiet på et tidligere tidspunkt.

Reason (1997) mente at menneskelige feil gjerne er et resultat av organisatoriske forhold som ofte baserer seg på beslutninger fra ledere (Reason, 1997, s. 11). Dersom ledere ikke prioriterer kunnskapsheving hos de ansatte, vil dette kunne resultere i feil. Et eksempel som gjerne trekkes frem er hvordan ansatte i virksomheter kan bli utsatt for sosial manipulasjon fra de datakriminelle. Sosial manipulasjon kan for eksempel skje gjennom falske e-poster og er en teknikk de kriminelle bruker for å påvirke en person til å utføre noe som ikke er i denne personens, eller virksomhetens beste interesse. Kostnadene for de datakriminelle ved å bruke slike metoder er lave, risikoen for dem er lav og det mulige utbyttet kan være svært høyt (Hadnagy, 2018, s. 7). Kunnskap og kompetanse hos de ansatte vil også kunne øke sensitiviteten til operasjoner og sette virksomheten i stand til å oppdage avvik mens de enda er sporbare og kan håndteres. Dette er viktig for de ansatte der arbeidet gjøres og krever oppmerksomhet, bevissthet til risiko og årvåkenhet (Weick & Sutcliffe, 2015, s. 77). Et eksempel her vil være å kunne skille mellom en falsk og ekte e-post og vite at virksomheten i det daglige kan bli utsatt for denne formen for trusler fra de datakriminelle. Aktive feil er feil begått av menneskene som jobber i virksomheten fra dag til dag (Reason, 1997) og dersom man er uheldig og for eksempel trykker på en falsk lenke eller vedlegg handler det om å forstå at det har skjedd og ta tak i det. Dette kan bidra til at virksomheten setter i gang med viktige tiltak, og oppretter kontakt med politiet for å avverge en mulig alvorlig situasjon.

God organisering, prosedyrer og rutiner blir trukket frem av begge utvalgene som sikkerhetstiltak som kun koster tid og planlegging sammenlignet med dyre teknologiske sikkerhetstiltak. Informantene fra utvalg 1 som jobber for en virksomhet som har fokusert på organisering, prosedyrer og rutiner dersom man blir utsatt for alvorlig datakriminalitet, ser nytten i å ha gjennomført dette arbeidet. Blant annet nevnes at kommunikasjonslinjene og rutinene når det kommer til samarbeid med politiet som viktige punkter.

> Teknologien som skal detektere og avverge trusler blir antakeligvis bare billigere og billigere, og da står du igjen med den ekstremt viktige funksjonen i slikt beredskapsarbeid, og det er organisasjonens evne til å håndtere krisen. Og det er ene og alene et spørsmål om organisering. Hvordan responderer vi når en sånn hendelse inntreffer, hvem gjør hva? Og det koster ikke penger. Det kan gjøres med den

> bemanningen man har, det krever bare kunnskap om god organisering (Kåre, Matproduksjon).

Organisering, prosedyrer og rutiner handler om hvordan en virksomhet forholder seg både i en før-, under- og etterkrisefase. Under selve krisen når virksomheten må mobilisere sin beredskap vil dette være sentrale momenter. Ifølge Turner (1978) kan ulykker skje på bakgrunn av hverdagslige prosesser i organisasjonen knyttet til for eksempel rutiner, prosedyrer og organisering. I etterkant av uønskede hendelser avdekkes det gjerne mangler når det kommer til virksomhetens evne til å forstå risiko, forebygge og håndtere de uønskede hendelsene. Dette viser viktigheten av en fornuftig organisering basert på god risikoforståelse i alle fasene av en krise. Turners syn på organisering, prosedyrer og rutinger kan på den måten ses i sammenheng med likhetsprinsippet som handler om at den organiseringen man opptrer med under kriser skal være likest mulig den organiseringen man har til daglig (Engen et al., 2021, s. 325). Likevel vil organiseringen under en krise være noe annerledes enn i det daglige. I teorien om høypålitelige organisasjoner er anerkjennelse av kompetanse et sentralt prinsipp. Ved å utnytte den kompetansen som er i virksomheten vil man kunne tilpasse seg komplekse settinger. Ved en uønsket hendelse som for eksempel alvorlig datakriminalitet er det ikke sikkert at det er virksomhetens ledelse som vil kunne ta de beste beslutningene, basert på kompetanse og erfaring. Her handler det også om å identifisere kompetanse og manglende kompetanse og se på hvordan man kan organisere seg best mulig under en hendelse (Weick & Sutcliffe, 2015, s. 116). Bevissthet rundt hvordan virksomheten er organisert og vil organisere seg under en krise, hvem som er sentrale personer med kompetanse og bevissthet rundt hva politiets rolle er og hva politiet kan bidra med i en krise knyttet til alvorlig datakriminalitet, vil være viktig for samarbeidet mellom virksomhetene og politiet. Det handler om å kunne tilpasse seg situasjonen og på best mulig måte dra nytte av den kompetansen som eksisterer for å håndtere hendelsen på best mulig måte. I tillegg trekker informanter fra utvalg 2 frem rutiner og prosedyrer knyttet til hvordan og når virksomheten kontakter politiet og hvordan de legger til rette for at politiet skal kunne gjøre sin jobb som viktig. Flere av informantene fra utvalg 1 forteller at politiets kompetanse når det kommer til krisehåndtering er en kompetanse som ikke så mange av virksomhetene har, og i et samarbeid med politiet vil denne kompetansen og styringen gjerne tillegges stor verdi så lenge politiet ikke overstyrer virksomheten. Flere av informantene som har erfaring fra samarbeid med politiet fra en reell hendelse hadde gode opplevelser med hendelseshåndteringen og hvordan arbeidet ble organisert. Likevel nevner også noen av informantene at noen virksomheter er usikre på hvor

stor kontroll politiet vil ta i en eventuell situasjon og overstyre virksomhetens organisering, og hvorvidt politifolk evner å sette seg inn i sentrale momenter ved virksomhetsstyring som er viktige å ha i bakhodet under en alvorlig hendelse.

Beredskapsplaner kan som nevnt testes gjennom mobilisering ved en reell uønsket hendelse eller ved trening og øving. Flere av informantene i utvalg 1 forteller at de har gjennomført beredskapsøvelser knyttet til alvorlig datakriminalitet som for eksempel et dataangrep. Tanken om hva som skjer dersom alle systemene til virksomheten ikke fungerer eller er tilgjengelig for virksomheten har blitt et populært utgangspunkt etter angrepet mot Hydro i 2019. Informantene fra utvalg 1 som enten har opplevd en krise knyttet til datakriminalitet eller som har erfaring fra trening og øving, forteller at den kunnskapen og læringen virksomheten fikk ut av dette har vært essensiell i beredskapsarbeidet. Beredskapsplanene blir videreutviklet og forbedret og at virksomheten kan dra nytte av en økt effektivitet og mer koordinert organisering og hendelseshåndtering som et resultat av at man har forsøkt å gjennomføre det i praksis. I tillegg har de opplevd at den kollektive risikoforståelsen og bevisstheten i virksomheten har økt og at treningen og øvingen har bidratt til å styrke fokuset på sikkerhet og sikkerhetskulturen. Det blir liksom mer realistisk og nært når man har opplevd noe i praksis. Dette har også ført til at kontakt med politiet og andre myndigheter har blitt enklere nettopp fordi det er tatt stilling til og prøvd ut.

> Skal man få til god hendelseshåndtering, og det gjelder i alt sikkerhetsarbeid, så må man være trent og ha øvd på det. Og i det så ligger det et godt planverk. Det er liksom ryggmargen (Kristoffer, Politi- og lensmannsetaten).

Resiliens handler om evnen til tilpasning når noe uforutsett skjer og etablerte rutiner og prosedyrer er mangelfulle, noe som kjennetegner høypålitelige organisasjoner. Resiliens kan også handle om evnen til læring og vokse seg sterkere gjennom en krise eller en fiktiv krisesituasjon. Virksomhetene må i en krisesituasjon raskt og effektivt tilpasse seg en ny og uventet situasjon og er avhengig av en koordinert mobilisering og god kollektiv situasjonsforståelse (Engen et al., 2021, s. 172). Det vil kunne være utfordrende for en virksomhet som ikke har trent på å mobilisere beredskapsorganisasjonen i en reell krisesituasjon. Det kan tenkes at det vil bli et ekstra stressmoment i tillegg til en allerede svært usikker og kompleks situasjon. Dersom virksomheten som et utgangspunkt har med i sitt beredskapsplanverk at de skal kontakte politiet, kan det plutselig oppstå utfordringer rundt dette fordi virksomheten kanskje ikke vet hvem i politiet, eller hvordan man kommer i kontakt med de riktige polititjenestepersonene eller hvilken informasjon politiet trenger. Trening og

øving blir et sikkerhetstiltak i den forstand at det vil kunne øke virksomhetens evne til å respondere på en effektiv og god måte på en uønsket hendelse, i tillegg til at trening og øving vil kunne bidra til å øke bevissthet og forståelse for de ansatte (Reason, 1997).

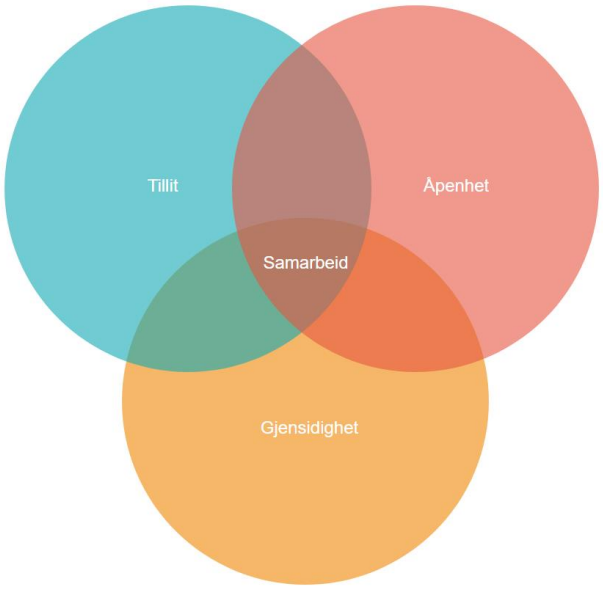
Trening og øving vil også kunne avdekke feil og mangler i beredskapsplanverket og forhindre «fantasidokumenter» og symbolsk sikkerhet som nevnt tidligere. Turner (1978) var opptatt av læring og utvikling i organisasjoner. Trening og øving vil kunne gjøre at virksomhetene lærer av feil og kan utvikle beredskapsplanene, organiseringen, rutinene og prosedyrene, også når det kommer til samarbeid med politiet. Trening og øving er også i tråd med samvirkeprinsippet ved at virksomheten har et selvstendig ansvar for å sikre best mulig samvirke med relevante aktører (Engen et al., 2021, s. 325). Dette kan også ses i sammenheng med samstyring som ifølge Røiseland og Vabo (2012) er en ikke-hierarkisk prosess der offentlige og private aktører og ressurser koordineres for å drive risikostyring, beredskapsarbeid og hendelseshåndtering (Røiseland & Vabo, 2012, referert i Engen et al., 2021, s. 213). Forpliktelse til resiliens er et sentralt prinsipp i teorien om høypålitelige organisasjoner. Også her fokuseres det på at virksomheten må lære av sine feil og tilpasse seg en uventet og uønsket situasjon for å håndtere denne på best mulig måte for så å komme styrket ut i den andre enden og raskt kunne fortsette sin virksomhet. I tillegg må virksomheten utfordre sine oppfatninger (Weick & Sutcliffe, 2015, s. 96). Det å være tilpasningsdyktig, evne og omstille seg og lære av praksis står sentralt når det kommer til trening og øving. Politiet kan ikke komme inn i en situasjon og «fikse alt» for en virksomhet som står i en krise. Samarbeidet kan tenkes å bli best i en situasjon hvor virksomheten har erfaring med å omstille seg og på denne måten kan det også tenkes at de får mest ut av et samarbeid med politiet. I trening og øving kan det også ligge at virksomhetene kontakter politiet hvor man i ro og mak kan etablere kontakt og gå opp linjene for samarbeidet.

5.3 Samvirke

Samarbeidet mellom de norske virksomhetene og politiet har nå blitt drøftet opp mot menneskelige og organisatoriske forhold i virksomhetene, knyttet til sentrale beredskapsteorier. Jeg vil nå se nærmere på hvordan politiets arbeid med datakriminalitet påvirker samarbeidet mellom virksomhetene og politiet. Dette vil i all hovedsak bli drøftet opp mot temaene tillit, åpenhet og gjensidighet.

Samfunnets avhengighet av IKT gjør det nødvendig med et godt samarbeid mellom norske virksomheter og offentlige myndigheter. Verken myndighetene, næringslivet eller

enkeltpersoner kan møte utfordringene i det digitale rom alene. Samarbeidet må rettes mot å forebygge, avdekke og håndtere datakriminalitet og uønskede digitale hendelser. Samarbeidet mellom norske virksomheter, politiet og andre offentlige myndigheter vil kunne bidra til bedre risikoforståelse, beslutninger og ressursutnyttelse (Meld. St. 38, (2016-2017), s. 19; NSM, 2021, s. 10). Blant de overordnede målene i nasjonal strategi for digital sikkerhet finner vi målet om at norske virksomheter digitaliserer på en sikker og tillitsvekkende måte og har bedre evne til egenbeskyttelse mot datakriminalitet og uønskede digitale hendelser. Et annet overordnet mål er at politiet skal styrke sin evne til å bekjempe datakriminalitet. De styrende prinsippene som gjelder disse målene, omhandler samarbeid mellom næringslivet og myndighetene. Samarbeidet skal blant annet føre til å identifisere, utveksle erfaringer og drøfte digitale sikkerhetsutfordringer, det skal være forpliktende for begge parter og være basert på åpenhet, tillit og gjensidighet (Departementene, 2019, s.7-9). Figur 5.2 viser relasjonen mellom tillit, åpenhet og gjensidighet i samarbeidet mellom de norske virksomhetene og politiet, og hvordan disse påvirker hverandre.



Figur 5.3 Relasjon mellom tillit, åpenhet og gjensidighet i samarbeidet mellom virksomhetene og politiet.

5.3.1 Tillit

Befolkningens tillit til sentrale samfunnsinstitusjoner er viktig for deres funksjonalitet, spesielt i forbindelse med kriser (Kruke, 2009, referert i Engen et al., 2021, s. 370). Det er viktig for myndighetene å synliggjøre at datasikkerhet tas på alvor for å opprettholde legitimiteten og tilliten befolkningen har til offentlige institusjoner (Engen et al., 2021, s.

252). Tillit har en tendens til å fremkalle mer tillit, og mistillit gjerne fremkaller mer mistillit (Fox, 1974, referert i Engen et al., 2021, s. 371). Mistillit kan oppstå på bakgrunn av tiltak ulike aktører tar eller ikke tar og vi forholder oss gjerne til aktører vi kan stole på (Cook mfl., 2005, referert i Engen et al., 2021, s. 371). Samarbeid og samhandling på tvers av fagområder i politiet, samt med aktører utenfor politiet, bidrar til en helhetlig tilnærming til politiets samfunnsoppdrag og kan gi store gevinster. Dette er også en avgjørende suksessfaktor for å skape et kunnskapsbasert politi. Politiet må samarbeide aktivt med andre offentlige aktører, næringsliv, frivillige organisasjoner og sivilsamfunnet ellers. Dette er viktig for det tillitsskapende arbeidet og som et fundament for det kunnskapsbaserte politiarbeidet (POD, 2020, s. 17). Flere av informantene i utvalg 2 mener at politiet har kommet sent på banen når det kommer til datakriminalitet, noe som har gjort at andre, både offentlige og private aktører, har tatt et ansvar som politiet burde tatt. Dette bryter med ansvarsprinsippet, da politiet ikke har tatt tilstrekkelig ansvar for datakriminalitet som er en tydelig del av politiets mandat (Engen et al., 2021, s. 325). Det kan med dette tenkes at mange virksomheter har utviklet et tillitsforhold til andre aktører enn politiet i forbindelse med utfordringene knyttet til datakriminalitet når politiet ikke har kunnet tilby de tjenestene som er forventet. Flere av informantene i utvalg 1 forteller at de ikke alltid assosierer datakriminalitet med politiet fordi politiet ikke har tatt nok ansvar og vært synlige nok. Samtidig kan det tenkes at virksomhetenes risikoforståelse knyttet til at uønskede digitale hendelser har spilt inn på deres forståelse av hvilke offentlige myndigheter det er riktig å henvende seg til, da de ikke har ansett dette som kriminalitet (Engen et al., 2021, s. 92; Aven et al., 2019, s. 40). Flere av informantene i utvalg 1 forteller om et godt samarbeid med for eksempel NSM, som har kommet tidligere på banen enn politiet når det kommer til datakriminalitet og digitale uønskede hendelser. Det er en viss overlapp mellom mandatet til politiet og andre aktører som NSM, noe som også kanskje bidra til at virksomhetene opplever at de samarbeider med rett aktør, og at tilliten styrkes gjennom at de får god hjelp. Likevel er informantene i utvalg 1 tydelige på at de savner mer tilstedeværelse fra politiet og et økt samarbeid da forståelsen for og fokuset på at digitale uønskede hendelser faktisk er kriminalitet på linje med annen kriminalitet har økt, noe som tydeliggjør politiets ansvar.

Som tidligere nevnt viste mørketallsundersøkelsen (2020) at kun 11% av virksomhetene som deltok i undersøkelsen rapporterte datakriminalitet til politiet (NSR, 2020). Informantene med tilknytning til politi- og lensmannsetaten fortalte om forebygging som politiets hovedstrategi og at politiet har skjønt at å «etterforske seg ut» av datakriminaliteten ikke er

veien å gå. Det handler heller om å sette virksomhetene i stand til å beskytte seg selv gjennom det forebyggende arbeidet noe som er i tråd med politiets forebyggende strategi (POD, 2020, s. 8-9). I Politidirektoratets rapport *Trusler og utfordringer innen IKT-kriminalitet* (2017) trekkes blant annet elementer ved datakriminalitet som kompleksitet, informasjonstilgang og datalagring, utenlandske aktører, bruk av kryptovaluta og krypteringsløsninger innen kommunikasjon frem som utfordringer for politiet når det kommer til politiets evne til å avdekke og etterforske kriminaliteten. Videre nevnes det i rapporten at mørketallene er store og at det er viktig at datakriminalitet blir anmeldt slik at politiet kan målrette sin innsats mot datakriminalitet basert på et kunnskapsgrunnlag. Det nevnes også at tilrettelegges for at datakriminalitet registreres på en effektiv og hensiktsmessig måte (POD, 2017, s. 26). I Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT (2021) kommer det frem at politiets evne til å avdekke og oppklare datakriminalitet har klare svakheter og samlet sett er alvorlige. Dette baserer seg på en manglende kompetanse, kapasitet, oversikt over datakriminaliteten, lav prioritering av datakriminalitet både av politiet, Politidirektoratet og Justis- og beredskapsdepartementet (Riksrevisjonen, 2021, s. 5). Informantene i utvalg 2 forteller om utfordringer når det kommer til kapasitet og kompetanse innen datakriminalitet i politiet, og fremhever også at det er store forskjeller innad i politiet. Den manglende kompetansen og kapasiteten gjør at virksomhetene ikke har en garanti for å få god hjelp dersom de kontakter politiet, i tillegg til at det er få distrikter som er kapable til å etterforske datakriminalitet alene. Dette handler om en kombinasjon av politiets kompetanse og kapasitet, og at datakriminalitet ofte er store, komplekse og krever mye kapasitet for å etterforske. Flere av informantene i utvalg 1 er usikre på hvordan politiet jobber med datakriminalitet og hvilken kompetanse de kan forvente å møte dersom de kontakter politiet. Det er også varierende hvorvidt virksomhetene faktisks har tillit til at de vil få hjelp og om det er noe poeng i det hele tatt å levere anmeldelser og informasjon om datakriminalitet. Mange tenker at dette kun blir for å bidra til et statistisk grunnlag. Flere av informantene forteller at virksomhetene de jobber for har opplevd at når de kontakter politiet for å anmelde, til og med i store saker, ender det kanskje bare med henleggelser. Kontakt med politiet blir også trukket frem som noe som spiller inn på tilliten og samarbeidet. Flere av informantene forteller om uheldige opplevelser når de har kontaktet politiet, noe som har ført til en svekket tillit.

> Politiet har bygget et ganske robust kompetansesenter på Kripos, det som skalles NC3. Men det politiet som virksomhetene møter ute, det er de lokale politidistriktene, og der har vi en lang vei å gå. Jeg har vært borti virksomheter som har kontaktet lokalt politi

> for å anmelde også blir de sendt hjem igjen. Dette er jo noe vi må ta innover oss når vi driver og oppmuntrer virksomhetene til å anmelde, så er det jo gjerne lokalt politi som de møter, og da er det ikke sikkert de vil bli ivaretatt på en god måte når det kommer til datakriminalitet altså (Ruben, Politi- og lensmannsetaten).

Politiet er avhengig av tillit for å kunne ivareta samfunnsoppdraget på en god måte. Tilliten til politiet påvirkes av hvor effektivt og kompetent politiet er til å løse sine oppgaver, samt hvordan politiet opptrer i oppgaveløsningen (POD, 2020, s. 19). Riksrevisjonen mener det er alvorlig at det ikke er tatt tilstrekkelige grep for å styrke politiets kompetanse og kapasitet når det kommer til datakriminalitet. Dette vil kunne føre til at politiet mister tillit hos virksomhetene (Riksrevisjonen, 2021, s. 6). Begge intervjuutvalgene trekker frem at politiets manglende kapasitet og kompetanse når det kommer til datakriminalitet både har og vil kunne påvirke samarbeidet mellom virksomhetene og politiet negativt. En vanlig grunn til at virksomheter ikke rapporterer eller involverer politiet og andre myndigheter når det kommer til datakriminalitet er at politiet ikke har kompetanse og kapasitet til å stille med en effektiv respons (Kennedy, 2016; Taylor, 2002, referert i Kemp et al, 2022, s. 4*).* Blant informantene er det tydelig at dette ikke handler om en motvilje til å samarbeide, tvert imot. Det er tydelig at det er et stort ønske om å få etablert et velfungerende samarbeid. Likevel kan en svekket tillit gjøre dette vanskelig å få til. Samtidig som det er et stort fokus på politiets manglende kapasitet og kompetanse er det tydelig at informantene i utvalg 1 er positive til de fremskrittene politiet har hatt de siste årene, og flere viser til at politiets arbeid med Hydrosaken har bidratt til å skape håp for politiets arbeid med datakriminalitet.

5.3.2 Åpenhet

For å bedre samarbeidet mellom virksomhetene og politiet kan det være viktig å se på hva som ligger bak virksomhetenes valg om å være åpne om at de har blitt utsatt for datakriminalitet og hvorvidt de deler informasjon om dette med politiet (Kemp et al., 2022, s. 2). Åpenhet rundt hendelser og informasjonsdeling vil kunne føre til økt bevisstgjøring generelt i samfunnet, men også for politiet og andre myndigheters kunnskapsgrunnlag (NSM, 2021, s. 31; POD, 2017, s. 26). I politiets forebyggende strategi (2021-2025) pekes det på at politiets virksomhet må utvikles på grunnlag av kunnskap om kriminalitetsutviklingen (POD, 2020, s. 13). I en artikkel publisert på NSM sine nettsider i 2020 kom det frem at NSM har erfart at mange virksomheter ikke ønsker å offentliggjøre eller anmelde at de har blitt utsatt for datakriminalitet, og det pekes på at årsakene til å ikke offentliggjøre kan være komplekse.

Videre pekes det på at det kan være gode grunner til å vente med å offentliggjøre situasjonen, men at det likevel er viktig å dele informasjon med myndigheter og andre viktige samarbeidspartnere raskt (Thon, 2020). Åpenhet rundt datakriminalitet har vært et tema i flere av NSMs årlige rapporter om det digitale risikobildet (NSM, 2019; NSM, 2020; NSM, 2021).

Liten åpenhet om alvorlig datakriminalitet kan knyttes til usikkerhet rundt negativ publisitet og lav tiltro til politiet. Bergsjø og Windvik (2018) viser til mørketallsundersøkelsen gjennomført av NSR og knytter lav rapportering av datakriminalitet til at politiet ikke har kompetanse og kapasitet til å etterforske datakriminalitet (Bergsjø & Windvik, 2018, s. 196; Riksrevisjonen, 2021). Aakre (2020) forklarer i sin rapport grunnene til at få virksomheter anmelder kan være manglende bevissthet rundt hva som er en kriminell handling, og at politiet ikke har ressurser og kompetanse til å følge opp (Aakre, 2020. s. 23). Informantene fra begge utvalg forteller om politiets manglende kompetanse og kapasitet, noe som også er et sentralt tema i Riksrevisjonens gjennomgang av politiets håndtering av IKT-kriminalitet (Riksrevisjonen, 2021). Dette bryter også med prinsippet om samvirke hvor virksomheten har et selvstendig ansvar for å sikre best mulig samvirke med relevante aktører. Dersom politiets kompetanse og kapasitet når det kommer til datakriminalitet er lav vil dette kunne spille inn på hvor relevant politiet anses som aktør og samarbeidspartner av virksomhetene (Engen et al., 2021, s. 325). At politiet har manglende kompetanse og kapasitet vil kunne lede til at virksomhetene ikke deler informasjon med politiet, men kanskje heller med andre myndighetsaktører som de anser som mer kompetente til å bistå dem, som for eksempel NSM. Dette er i tråd med teorien om høypålitelige organisasjoner og prinsippet om anerkjennelse av kompetanse, hvor virksomhetene vil forsøke å øke egen kompetanse gjennom andre i tillegg til å be om bistand fra eksterne eksperter (Weick & Sutcliffe, 2015). Når det kommer til hva som anses eller oppfattes som en kriminell handling kan dette ses i sammenheng med vår risikoforståelse (Engen et al., 2021, s. 92; Aven et al., 2019, s. 40). Dersom virksomheten ikke anser uønskede digitale hendelser, mindre alvorlige eller alvorlige, som datakriminalitet kan dette spille inn på deres åpenhet og fokus på informasjonsdeling med politiet. Samtidig ville det være kritikkverdig om virksomheter i dag ikke har fått med seg at truslene fra datakriminelle og det digitale rom er datakriminalitet. I den sammenheng kan kanskje en manglende åpenhet og informasjonsdeling med politiet knyttes til virksomhetens digitale sikkerhetskultur og ledelsens prioritering og fokus på truslene (Reason, 1997; Weick & Sutcliffe, 2015; Turner, 1978).

Negativ publisitet, altså hvordan åpenhet om at virksomheten har blitt utsatt for datakriminalitet kan spille inn på virksomhetens omdømme, var et sentralt tema hos begge intervjuutvalgene. I utvalg 2 forteller flere av informantene at de opplever at virksomhetenes åpenhet har nær tilknytning til virksomhetenes omdømme. Informantene har flere eksempler på virksomheter som har hold dataangrep skjult, noe de forklarer med at virksomhetene kanskje er flaue over dårlig sikkerhet eller at de er redde for at dersom informasjonen kommer ut vil dette kunne påvirke virksomhetens omdømme negativt og ha konsekvenser for virksomhetens videre drift. Lagazio et al. (2014) mente at en av hovedårsakene til at virksomheter ikke anmelder datakriminalitet er å forhindre skade på virksomhetens omdømme i den forstand at kunder taper tillit til virksomheten (Lagazio et al., 2014, referert i Kemp et al., 2021, s. 5). Likevel peker flere av informantene på at virksomheter som velger å være åpne og som velger å dele informasjon med politiet ofte kommer veldig bra ut av en slik krise. Flere av informantene i utvalg 1 trekker også frem at det å være redd for at åpenhet og det å involvere politiet kanskje skal skade omdømmet gjaldt mer for noen år tilbake. Dette handler mulig om at flere virksomheter har vært åpne noe som er med på å senke terskelen for andre, i tillegg er det så vanlig at virksomheter på ett eller annet tidspunkt blir angrepet. Det er vanlig at virksomheter vil kunne se en innvirkning på omdømme gjennom tap av tillit rett i etterkant av en krise. Likevel er det ikke sånn at dette vil være vedvarende. Sentralt i det å komme seg fra en uønsket hendelse og gjenvinne tillit og produksjon er virksomhetens og ledelsens krisekommunikasjon og evne til å være åpen og ærlig. Dette vil vise virksomhetens evne til å håndtere en vanskelig situasjon og egner seg til å gjenvinne tillitt og opprettholde virksomhetens omdømme (Knight & Pretty, 2001, s. 15).

Kristoffer, fra politi- og lensmannsetaten, forteller også at han tror dette med omdømme kan gå to veier når det kommer til samarbeid med politiet. Noen virksomheter vil ønske å ikke dele informasjon og være åpne fordi de tenker at det vil kunne svekke omdømmet gjennom at dårlig datasikkerhet osv. kanskje vil bli avslørt, mens andre involverer politiet helt bevisst for å styrke omdømmet og vise at de tar situasjonen seriøst og ønsker å bidra til å bekjempe datakriminalitet, og noen fordi de trenger hjelp. Thon (2020) mener at god krisekommunikasjon har større betydning for omdømme enn det faktum at virksomheten er rammet av et dataangrep. Han mener at måten Hydro valgte å kommunisere på under dataangrepet 2019 er et godt eksempel på hvordan god krisekommunikasjon kan bevare omdømmet til virksomheten og gjenoppbygge tillit (Thon, 2020; Olsen & Mathiesen, 2019, s.193; Engen et al., 2021, s. 369). Informanter fra begge utvalgene trekker frem Hydros

åpenhet rundt dataangrepet som noe som har bidratt til at virksomhetene har fått et annet syn på dette med åpenhet og samarbeid med politiet.

Virksomheter som prioriterer digital sikkerhet høyt har større sannsynlighet for å være åpne og involvere politiet og andre offentlige myndigheter enn virksomheter som ikke prioriterer dette arbeidet (Kemp et al., 2021, s. 14). NSM opplever at virksomheter i økende grad er åpne om at de har vært utsatt for uønskede digitale hendelser og deler sine erfaringer, noe som kan ha sammenheng med at fokuset norske virksomheter har på å inkludere digital sikkerhet i beredskapsarbeidet har økt de siste årene (NSM, 2021, s. 31). Virksomheter som gjennomfører god styring og ledelse innen datasikkerhet og har gode beredskapsplaner og trener, rapporterer oftere datakriminalitet til politiet (Wanamaker, 2019, referert i Kemp et al, 22, s. 5). Flere av informantene i utvalg 1 forteller om hvordan kontakt med politiet er en sentral del av beredskapsplanene og noe som de har diskutert med ledelsen. De kaller dette «regler om åpenhet», «policy» og «rutiner» og «nulltoleranse». I utvalg 2 forteller flere av informantene at dersom kontakt med politiet er en del av beredskapsplanene vil dette påvirke hva som faktisk gjøres når virksomhetene først har vært uheldige. Samtidig som flere av informantene i utvalg 1 forteller om at det å kontakte politiet dersom de hadde blitt utsatt for datakriminalitet hadde vært helt naturlig, er det flere som forteller at dette må vurderes i hver enkelt situasjon. Dette knytter de til et behov for å ha kontroll på situasjonen før de kan vurdere å gå til politiet. Oppfattelsen av at virksomhetene ikke alltid følger policyene om å være åpne om datakriminalitet og dele informasjon med politiet trekkes også frem av informantene i utvalg 2. Det fremstilles som en opplevelse av at virksomhetene ønsker å ha handlingsalternativer, og at de mister dette dersom de kontakter politiet. Derfor vil virksomhetene kunne se bort fra beredskapsplanene når noe skjer for å kunne gjøre en situasjonsbestemt vurdering og opprettholde handlingsalternativene. Naturlig nok vil virksomhetene prioritere å gjenoppta sikker drift av selskapet og i noen tilfeller vil kanskje noen velge for eksempel å betale et løsepengevirus for å nettopp få opp produksjonen igjen. Intervjuobjektene i utvalg 2 forteller også om virksomheter som har kontaktet politiet etter at de har betalt et løsepengekrav fordi det ikke ga det resultatet de ønsket. Her kan det tenkes at ledelsens forpliktelse og opptatthet av sikkerhet vil kunne ha mye å si for hvordan virksomheten forholder seg til å kontakte politiet når en uønsket hendelse skjer, sammen med hvilken risikoforståelse og sikkerhetskultur som er etablert i virksomheten (Turner, 1978; Reason, 1997). Dersom ledelsen er tilbakeholden og ønsker å «se an» situasjonen vil dette kunne bidra til en kultur hvor det å være åpen og dele informasjon med politiet og andre

relevante myndigheter ikke forstås som så viktig. Flere av informantene i utvalg 2 forteller om viktigheten av tidlig involvering og informasjonsdeling for at virksomhetene skal kunne få god hjelp av myndighetene og at man potensielt vil kunne bidra med god beslutningsstøtte i en kaotisk situasjon, og mulig vil kunne avverge at en uønsket hendelse skjer andre.

Oppfatningen om at det bare er virksomheter som har dårlig datasikkerhet som blir offer for datakriminalitet må endres. Datakriminalitet vil før eller siden ramme alle virksomheter, uavhengig av om sikkerheten er god eller dårlig. God datasikkerhet vil likevel redusere risikoen for at noe skjer, og setter virksomhetene i bedre stand til å redusere konsekvensene dersom en uønsket hendelse inntreffer (Thon, 2020). Flere av informantene i utvalg 1 fortalte om en følelse av at det kun er et spørsmål om tid før virksomheten de jobber for blir utsatt for alvorlig datakriminalitet. Dette baserer seg på at man ser at metodene som brukes av de kriminelle aktørene er så profesjonelle og sofistikerte at det ikke alltid handler om hvor gode tekniske sikkerhetsløsninger en virksomhet har eller hvor godt organisert man er. Dersom de kriminelle er gode nok, kommer de seg inn. Dette viser at mange av informantene i utvalg 1 representerer en virksomhet som har tatt høyde for trusselen fra datakriminelle og det digitale rom i sin risikoforståelse (Engen et al., 2021, s. 92; Aven et al., 2019, s. 40). Flere av informantene i utvalg 1 forteller også om at fokuset på og prioriteringen av digital sikkerhet har fått mer oppmerksomhet fra ledelsen og at den digitale sikkerhetskulturen har blitt betraktelig bedre (Turner, 1978; Reason, 1997).

Virksomhetens valg om å være åpen og dele informasjon med politiet kan avhenge av virksomhetens evne til å håndtere problemet internt eller gjennom et privat hendelseshåndteringsselskap (Wanamaker, 2019, referert i Kemp et al., 2022, s. 4). I tillegg vil virksomhetens vurdering rundt forhold til kunder eller stakeholders og deres tillit til virksomheten kunne spille inn på vurderingen rundt åpenhet og involvering av politiet (Lagazio et al, 2014, referert i Kemp et al, 2022, s. 5). Informanter fra begge utvalg forteller om at virksomhetene har en kompleks målgruppe å forholde seg til, noe som kan spille inn på hvordan virksomheten håndterer åpenhet om datakriminalitet og involvering av politiet. Informanter fra utvalg 1 trekker inn at det er viktig for dem å kunne samarbeide med politiet uten at informasjonen «lekker» og det blir gjort til noe større enn det trenger å være. Informanter fra utvalg 1 forteller at dette i ytterste konsekvens kan føre til at virksomheten mister kontakter og relasjoner. Det trekkes frem at virksomhetene ikke ønsker å «bekymre» stakeholderne sine unødvendig, spesielt i en innledende fase av en uønsket hendelse når det er mye usikkerhet. Dette utløser også et behov for virksomhetene for å styre den informasjonen

som kommer ut. I denne sammenheng er flere av informantene opptatte av å forklare at politiets samarbeid i denne sammenheng er viktig og at politiet må respektere virksomhetenes behov. Det vil være en avgjørende faktor for åpenhet og involvering av politiet. Informanter fra utvalg 2 som har tilknytning til politi- og lensmannsetaten forteller at de har opplevelser med at noen virksomheter tror at dersom de kommer til politiet med noe så er det ensbetydende med at informasjonen blir offentlig kjent og at det kommer ut at virksomheten har blitt utsatt for noe. Informantene i utvalg 1 forteller at det er helt avgjørende i samarbeidet med virksomhetene at politiet og myndighetene har et godt tillitsforhold med virksomhetene.

Flere informanter i utvalg 1 forteller at de har opplevd at politiet ikke har et godt mottaksapparat for informasjonen de ønsker å dele. Dette dreier seg både om anmeldelser, tips og større mengder oppsamlet informasjon. Enkelhet og tilgjengelighet ble et sentralt tema i alle intervjuene, og mange av informantene i utvalg 1 uttrykte frustrasjon over at politiet ikke har evnet å etablere et godt mottaksapparat for henvendelser. Også informanter fra utvalg 2 trekker dette frem som et problem som har eksistert lenge. Likevel forteller informantene tilknyttet politi- og lensmannsetaten at dette begynner å ta form og at politiet i 2021 lanserte en digital tipsfunksjon. Likevel er det fremdeles en vei å gå og at det er en bevissthet i politiet rundt dette problemet. Riksrevisjonen (2021) påpeker også at politiets evne til å ta imot informasjon om datakriminalitet fra virksomhetene er et problem. De knytter dette direkte til politiets kunnskapsgrunnlag. Politiet har over tid ikke hatt et tilfredsstillende kodeverk for datakriminaliteten, noe som gjør at politiet har manglet kontroll over datakriminaliteten (Riksrevisjonen, 2021). Informantene i utvalg 1 forteller at de gjerne skulle gitt fra seg mer informasjon om datakriminalitet, spesielt den mindre alvorlige datakriminaliteten, til politiet. De påpeker også at dersom løsningen for å anmelde datakriminalitet til politiet hadde blitt digitalisert og på den måten blitt både mer tilgjengelig og effektiv ville dette virket positivt på samarbeidet ved at virksomhetene i større grad hadde anmeldt.

Informantene i utvalg 1 forteller at politiets enkelhet og tilgjengelighet for kontakt er sentral når det kommer til vurderinger de gjør når det kommer til kost/nytte, tid og prioriteringer. I tillegg er det et moment at virksomhetene er interesserte i å kunne komme i kontakt med «riktig person» raskt, i stedet for å måtte gjennom en rekke personer som kanskje ikke forstår hva virksomheten trenger. Her blir næringslivskontaktene trukket frem som en god kilde til både informasjon og rask kontakt, og politiets gjennomgående kunnskap om datakriminalitet blir trukket frem som en utfordring fordi virksomhetene kan oppleve å komme i kontakt med en polititjenesteperson som ikke har god nok kunnskap verken til å

veilede, gi råd og bistå med viktige tiltak i en initialfase, og kanskje heller ikke gi informasjon om hvor virksomheten kan henvende seg. Kontakt og samarbeid med politiet vil også kunne bli nedprioritert dersom ikke virksomheten anser det som nyttig å kontakte politiet, eller ikke har tillit til at de vil få noe igjen. Likevel forteller virksomheter som har erfaring fra krisesituasjoner og samarbeid med politiet at den positive erfaringen fra samarbeidet har gjort et samarbeid og kontakt med politiet har havnet høyt opp på «prioriteringslisten» og er godt integrert i beredskapsplanene.

5.3.3 Gjensidighet

Politiet har behov for kunnskap om forhold som skaper eller kan skape kriminalitet eller uønskede hendelser, for å kunne gjøre de riktige prioriteringene og sette inn effektive tiltak som gir forebyggende effekt. Det må derfor være en kultur for å dele og utveksle kunnskap systematisk begge veier, og politiet må ha god samhandlingskompetanse. Gjennom god kommunikasjon, tilstedeværelse og tilgjengelighet kan politiet få kjennskap til publikums forventninger og behov, samt å formidle kunnskap og forebyggende råd (POD, 2020, s. 13-19). Gjensidighet vil her handle om den informasjons- og erfaringsutvekslingen som går fra virksomhetene til politiet og fra politiet til virksomhetene.

> Det første som slår meg når vi snakker om informasjonsdeling er «toveis». At vi ikke øser over alt vi har også får vi ingenting tilbake. Det vil være utfordrende og det vil ikke stimulere til samarbeid. Vi er store på sikkerhet og vi tar det seriøst og har et stort samfunnsansvar, så vil jo vi dele vi uansett hva vi får vi får tilbake. Men det vil likevel være mye mer nyttig, effektivt og gledelig å få noe tilbake (Ole Gunnar, Finans).

I underkapitlet om åpenhet ligger fokuset på virksomhetenes åpenhet og deling av informasjon med politiet og hvordan dette er viktig i det forebyggende arbeidet til politiet for å etablere et godt kunnskapsgrunnlag og gi politiet muligheten til å forebygge og håndtere datakriminalitet. Samtidig er det viktig i det forebyggende arbeidet at det eksisterer god kommunikasjon og deling av informasjon og erfaring også fra politiet til virksomhetene. At politiet deler kunnskap om kriminalitet og uønskede hendelser og gir forebyggende råd til innbyggerne, media, virksomheter og samarbeidsaktører er trukket frem som faktorer som vil styrke politiets forebyggende arbeid (POD, 2020, s. 14). Politiets deling av kunnskap og erfaring rundt datakriminalitet til virksomhetene vil kunne bidra til at virksomhetene kan etablere en bedre risikoforståelse for truslene fra datakriminelle og fra det digitale rom, noe som er viktig for virksomhetens beredskapsarbeid, prioritering og fokus. I dagens komplekse

og hurtig skiftende trusselbilde vil informasjon fra politiet også kunne bidra til å hjelpe virksomhetene med å basere beredskapsarbeidet sitt på et utvalg av informasjon. Dette er i tråd med Turners (1978) teori om menneskeskapte ulykker og menneskets begrensede rasjonalitet. Vår evne til å forutse fremtidige farer vil være kontekstuell og nært knyttet til den kollektive risikoforståelsen i virksomheten.

Tillit kan påvirkes av kommunikasjon mellom myndigheter og allmennheten (Engen et al., 2021, s. 62). Aakre (2020) viser til rapporter fra NSR, NSM og NorSIS og har funnet en bred enighet om at samarbeid, åpenhet og informasjonsutveksling mellom virksomheter og myndigheter er nødvendig for å møte cybertruslene, samtidig som rapportene viser en manglende åpenhet som går begge veier (NSR, 2018; NSR, 2019, NSM, 2019, NorSIS, 2018, referert i Aakre, 2020). Hybridundersøkelsen (2019) tar for seg truslene fra hybride operasjoner som cyberangrep, nettmanipulering og desinformasjon, understreker at virksomhetene ønsker økt åpenhet fra myndighetene om uønskede hendelser som myndighetene kjenner til. Over halvparten av virksomhetene i undersøkelsen svarer at de mener norske myndigheter bør bidra med mer informasjon, klarere retningslinjer, veiledning og åpenhet om hybride hendelser (NSR, 2019, s. 29). Flere av informantene fra utvalg 1 trekker frem at de ønsker mer informasjon om datakriminalitet fra politiet. De nevner både informasjon om trusselbildet gjennom informasjonsprodukter, næringslivskontakter, seminarer og gjennom media. Informasjon- og erfaringsutveksling fra politiet til virksomhetene vil kunne hjelpe virksomhetene til å etablere bedre risikoforståelse, noe som igjen kan spille inn på ledelsens prioritering av og fokus på digital sikkerhet. Dette vil kunne bidra til å etablere en bedre sikkerhetskultur i virksomheten, hvor forståelsen av kontakt med politiet er viktig når det kommer til forebygging og håndtering av datakriminalitet og uønskede digitale hendelser (Aven et al., 2019; Turner, 1978; Reason, 1997).

Når det kommer til å «få noe tilbake» nevner flere av informantene i utvalg 1 at de ønsker å bli tatt seriøst og bli møtt med råd og hjelp til hendelseshåndteringen dersom de kontakter politiet. Flere gir uttrykk for at de ikke nødvendigvis har forventninger til at politiet har informasjon som kan løse den situasjonen de står i, men de ønsker likevel å få råd og veiledning til hvordan de best kan drive sitt forebyggende arbeid og håndtere alvorlige uønskede hendelser. I teorien om høypålitelige organisasjoner vil denne typen kunnskap kunne bidra til at virksomhetene i større grad øker sin opptatthet av feil gjennom å kunne identifisere og håndtere små hendelser som dukker opp før de utløser en større hendelse, virksomheten kan motvirke å overforenkle årsaker gjennom å vite hva som kan forårsake feil

og uønskede digitale hendelser og de kan oppdage avvik mens de fremdeles er sporbare (Weick & Sutcliffe, 2015). Også informantene i utvalg 2 påpeker at politiet i større grad burde bidra med informasjon til virksomhetene om datakriminalitet, spesielt når det kommer til det forebyggende arbeidet, og informantene med tilknytning til politi- og lensmannsetaten forteller at de opplever at en av de viktigste årsakene til at virksomhetene kontakter politiet er for å få råd og hjelp til å løse situasjonen. Informanter fra utvalg 2 håper at virksomhetene vil komme til politiet, fordi politiet kan gi dem god beslutningsstøtte i de valgene de står ovenfor. Et eksempel på dette er at de datakriminelle har kjørt noe som kalles «dobbel utpressing», hvor virksomheten kanskje betaler, med de datakriminelle forblir i nettverket og presser virksomhetene for mer penger. Dette er informasjon politiet kunne gitt flere virksomheter underveis i hendelseshåndteringen dersom politiet hadde blitt involvert.

I utvalg 1 er det en tydelig usikkerhet hos mange av informantene når det kommer til hva virksomhetene skal anmelde og ikke, hvilken informasjon som egentlig er av interesse for politiet og flere av informantene forteller at de ikke opplever å ha god nok kunnskap om hvordan politiet jobber med datakriminalitet og hva politiet kan bidra med dersom virksomheten kontakter politiet når en uønsket hendelse har skjedd. Informantene i utvalg 2 forteller at politiet er avhengig av å få informasjon om datakriminalitet for å etablere et kunnskapsgrunnlag som kan brukes som grunnlag i det forebyggende arbeidet. Dette dreier seg både om generell informasjon om datakriminalitet, forekomst og mengde, og mer spesifikk informasjon om alvorlig datakriminalitet. Dette kan eksempelvis være om de kriminelle aktørenes fremgangsmåte og hva slags sårbarheter og programvare som blir utnyttet. På denne måten blir ikke bare informasjon om trusselbildet viktig, men også at politiet kommuniserer hvordan de jobber, hva de kan bidra med og hvem som er riktig å kontakte. Dette vil også kunne bidra til å endre på holdninger, antakelser og misoppfatninger hos virksomhetene om hvordan politiet jobber, noe som kan bidra til mer tillit, økt åpenhet og informasjonsdeling begge veier. I virksomheter kan det råde antakelser som styrer den kollektive oppmerksomheten og atferden (Turner, 1978). Dersom virksomheten antar at politiet ikke kan bidra med noe er det enkelt å ikke kontakte politiet eller nedprioritere dette.

«Anmeld alt alltid» er en frase som flere av informantene fra begge utvalg forteller om at skaper usikkerhet og er misvisende med tanke på politiets kompetanse og kapasitet. Informantene gir uttrykk for at det både kan skape frustrasjon og mistillit og at det kan svekke samarbeidet gjennom at politiet ikke fremstår profesjonelle. Informanter fra utvalg 2 forteller at politiet ikke er avhengig av at virksomhetene nødvendigvis anmelder datakriminaliteten,

men politiet er avhengig av informasjon om hva som skjer og hva virksomhetene blir utsatt for slik at politiet kan drive forebyggende arbeid. I politiets forebyggende strategi (2021-2015) kommer det frem at en av ambisjonene for å styrke forebyggingen er at politiet viser åpenhet og forklarer egen handlemåte og tiltak som iverksettes (POD, 2020, s. 19). Her vil politiets kommunikasjon til virksomhetene som gir en forventningsavklaring om hva slags informasjon politiet trenger, når det er viktig å dele informasjon til politiet og hva virksomhetene kan forvente i den andre enden svært viktig for å styrke tillit og samarbeid samt motivere for åpenhet og informasjonsdeling begge veier.

Begge utvalg forteller om at politiet ikke er synlige nok i mediebildet når det kommer til datakriminalitet, og at politiet kan ha mye å hente på å kommunisere sin rolle, fortelle om hvordan de jobber og ta eierskap til tematikken og mandatet sitt. «Solskinnshistorier» som politiets arbeid med Hydrosaken blir trukket frem som et eksempel på en sak i mediebildet som har gjort at mange av informantene i utvalg 1 har fått øynene opp for hva politiet kan få til, noe som kan motivere virksomhetene til informasjonsdeling og samarbeid. Dette vil kunne bidra til å etablere politiet som en relevant aktør å samarbeide med i tråd med prinsippet om samvirke (Engen et al., 2021, s. 325), samt å gjøre politiet til en naturlig aktør som kan bidra til at virksomhetene øker sin kompetanse når det kommer til digitalt sikkerhetsarbeid gjennom utarbeidelse av beredskapsplaner, rutiner og gjennom trening og øving (Weick & Sutcliffe, 2015; Reason, 1997).

5.4 Modenhet – Helhetlig tilnærming, samfunnsansvar og gjensidig avhengighet

Modenhet er et begrep som gikk igjen hos informanter fra begge intervjuutvalgene. Det har vært vanskelig å finne en god definisjon på modenhet i faglitteratur og teori knyttet til samfunnssikkerhet og beredskap. Flere private sikkerhetsselskaper og hendelseshåndteringsselskaper har definert begrepet modenhet i forbindelse med modenhetsmodeller. Modenhet defineres i denne sammenheng som en virksomhets grad av beredskap og evne til å redusere sårbarheter og trusler fra datakriminelle (RSI Security, 2020). Modenhet som begrep nevnes gjerne i sammenheng med en virksomhets kartlegging av fremdrift mot et mål, også kalt modenhetsmodeller. I hovedtrekk beskriver modenhetsmodellene egenskaper ved organisasjoner som man kan forvente å se i en virksomhet med en effektiv tilnærming til digital sikkerhet (NCSC, 2018). Det finnes mange forskjellige modenhetsmodeller, og flere av dem har sentrale likhetstrekk spesielt med tanke på hvilke momenter virksomhetens modenhet blir vurdert etter. Et eksempel på en

modenhetsmodell er Cyber Maturity Assessment (CMA) hvor seks jevnbyrdige områder analyseres for å kartlegge virksomhetens modenhetsnivå. Områdene kartlegger både mennesker, organisasjon og teknologi og inneholder følgende (1) Styring og ledelse, (2) Menneskelige faktorer, (3) Risikohåndtering, (4) Kontinuitet og kriseberedskap, (5) IT-drift og teknologi og (6) Etterlevelse av lover og regler (KPMG, 2016).

Dersom vi ser på modenhet ut fra definisjonen over og momenter som gjerne inngår i en modenhetsmodell, kan det trekkes paralleller til flere av de teoretiske momentene denne oppgaven bygger på. Turners teori om menneskeskapte ulykker (1978) og Reason sin teori om organisatoriske ulykker (1997) er teorier som forklarer hvorfor ulykker skjer. Sentralt i teoriene er risikoforståelse, sikkerhetskultur, ledelse, kunnskap og kompetanse. Mens Turner (1978) beskriver en ulykkes «inkubasjonstid», altså små hendelser og skjulte feil som skjer i en virksomhet og som leder opp til en ulykke, fokuserer Reason (1997) på latente forhold som er forhold i en organisasjon som kan skape ulykker. Dette kan for eksempel dreie seg om organisering, beslutninger, ledelse, prosedyrer og rutiner. Begge teoriene fokuserer på hva årsakene til en ulykke ser dette i en menneskelig, organisatorisk og teknologisk kontekst. Teorien om høypålitelige organisasjoner tar sikte på å se på hvordan en organisasjon kan unngå ulykker, og har på den måten et mer forebyggende perspektiv. I HRO-teorien vil en virksomhet kunne danne grunnlaget for en helhetlig tilnærming til sikkerhet og motstandsdyktighet gjennom mindful organizing og sensemaking, som er en prosess basert på persepsjon, erfaring og forventninger. Dette er en dynamisk og kontinuerlig prosess som hjelper virksomheten med å opprettholde sikker produksjon gjennom å både kunne forutse og eventuelt mestre uønskede hendelser. Dette kan virksomheten oppnå gjennom å være opptatt av feil, altså være opptatt av små feil og hendelser som dukker opp som kan være indikasjoner på noe som kan utvikle seg til en alvorlig situasjon, motvillighet til å overforenkle, altså forenkle årsaker og med dette ikke se detaljene i hva som forårsaker feil og uønskede hendelser, sensitivitet til operasjoner, altså oppdage avvik mens de fremdeles er sporbare og kan håndteres, forpliktelse til resiliens, altså at virksomheten lærer av sine feil, utfordrer sine oppfatninger og evner å opprettholde eller gjenoppta virksomhet etter en uønsket hendelse og anerkjenne kompetanse gjennom mangfold i ekspertise, tilpasning i komplekse settinger og på best mulig måte utnytte ekspertise ved uønskede hendelser (Weick & Sutcliffe, 2015). Også NorSIS sine åtte kjerneområder har likhetstrekk med elementer fra modenhetsmodeller og modenhetsbegrepet. Kjerneområdene handler om fellesskap, styring og kontroll, tillit,

risikooppfattelse, optimisme for teknologi og digitalisering, kompetanse, interesse for teknologi og IT og atferdsmønstre (NorSIS, 2016, referert i Bergsjø et al., 2020, s. 36).

I teorien jeg har benyttet i denne oppgaven har menneskelige og organisatoriske forhold vært sentralt. Både elementer som inngår i modenhetsmodellene og i modenhetsbegrepet og det som ligger til grunn for de sentrale teoriene innen samfunnssikkerhet og beredskap fokuserer på en helhet når det kommer til arbeid med sikkerhet. En virksomhet kan ikke kun belage seg på dyre tekniske løsninger eller på gode beredskapsplaner. Ledelsen kan ikke la noen andre ta seg av sikkerheten og ikke ta del i arbeidet med dette. Sikkerhetskulturen blir ikke til av seg selv, og for å etablere god risikoforståelse kreves det kunnskap og kompetanse. Hvor moden en virksomhet er når det kommer til tematikken datakriminalitet og digital sikkerhet vil på denne måten kunne ses på som en sammensetning av flere faktorer som danner en helhet. Det handler blant annet om risikoforståelse, sikkerhetskultur, aksept for den trusselen datakriminalitet utgjør, kunnskap og kompetanse, hvordan en virksomhet jobber med en kontinuerlig utvikling og forbedring av sin beredskap gjennom planer, rutiner og trening og hvor godt sikkerhetsarbeidet er forankret i ledelsen. På denne måten vil en helhetlig tilnærming til sikkerhet gjenspeile virksomhetens modenhet.

Flere av informantene i begge utvalg fortalte om virksomhetenes samfunnsansvar når det kommer til digital sikkerhet og datakriminalitet. I et samfunn hvor virksomheter og funksjoner er tett sammenvevd og avhengig av hverandre, vil for eksempel et dataangrep mot en virksomhet kunne få store ringvirkninger og konsekvenser for også andre enn virksomheten selv (Aven et al., 2019, s. 21; Engen et al., 2021, s. 128). Viskosimeters valg om å involvere politiet gjennom anmeldelse, rapportering eller andre tilnærminger kan også knyttes til virksomhetens ønske om å hjelpe og bidra til et sikrere samfunn for alle (Bowles et al., 2009, referert i Kemp et al, 2022, s. 16). Å kontakte politiet og dele informasjon om datakriminalitet kan bidra til å øke bevisstheten i samfunnet og blant virksomheter, samt bidra til det forebyggende arbeidet (Laube & Böhme, 2016, referert i Kemp et al., 2021, s. 16; POD, 2020). På denne måten kan virksomhetenes valg om å prioritere det digitale sikkerhetsarbeidet også baseres på et ønske om å bidra til en større helhet gjennom å skape et tryggere samfunn (Kemp et al., 2022, s. 16). Dette er også i tråd med den nasjonale strategien om digital sikkerhet hvor det kommer frem at verken myndighetene eller virksomhetene kan håndtere truslene fra datakriminalitet og det digitale rom alene (Departementene, 2019).

At virksomhetene har et fokus på å ta samfunnsansvar kan også knyttes til virksomhetens modenhet. Flere av informantene i utvalg 1 forteller at deres virksomhet

kjenner på et samfunnsansvar. I dette legger de at ønsker å bidra til å forebygge og håndtere datakriminalitet ved å være åpne og dele informasjon med politiet om både mindre alvorlige og alvorlige tilfeller de er utsatt for. Flere uttrykker at de er bevisst at dersom deres virksomhet deler informasjon om for eksempel et dataangrep med politiet, kan dette bidra til at andre virksomheter kan unngå det samme angrepet. Selv om kanskje ikke politiet kan hjelpe virksomheten som har blitt utsatt for noe i det konkrete tilfellet, vil informasjonen kunne bidra til å hjelpe noen andre. Dersom alle har denne holdningen og tilnærmingen til den kollektive digitale sikkerheten vil politiet i større grad kunne hjelpe virksomhetene med å forebygge alvorlige hendelser. På samme måte vil informasjon om datakriminalitet kunne bidra til politiets kunnskapsgrunnlag, og politiet vil kunne bruke denne informasjonen til å informere om trusler og trender og gi råd og tips. Sett i sammenheng med krisens faser, vil politiet i en førkrisefase bidra til virksomhetenes beredskapsarbeid. Under en krise vil politiet kunne bidra med beslutningsstøtte gjennom å dele informasjon og erfaringer og hjelpe virksomhetene i håndteringen av hendelsen. I etterkrisefasen vil politiet kunne se på hva som skjedde for å lære av dette og dele informasjonen med virksomhetene slik at man kan dra nytte av hverandres feil og bruke dette videre i beredskapsarbeidet (Engen et al., 2021, s. 324; POD, 2020, s. 8-9).

> Dersom min virksomhet ble utsatt for noe og vi gikk til politiet så bidrar det til at flere, hvertfall da de ansatte i virksomheten, forstår at det er politiet vi skal gå til. Og det vil jo kunne fungere selvforsterkende greie, og igjen så mener jo jeg at når vi alle kan være enige om at det er ikke «top of the mind», at vi må jo starte med oss selv og ta ansvar for å være åpne, dele og samarbeide. Det vil ikke hjelpe at vi lar være fordi andre gjør det. Det vil jo være en helt meningsløs tilnærming (Stian, Teknologi og innovasjon).

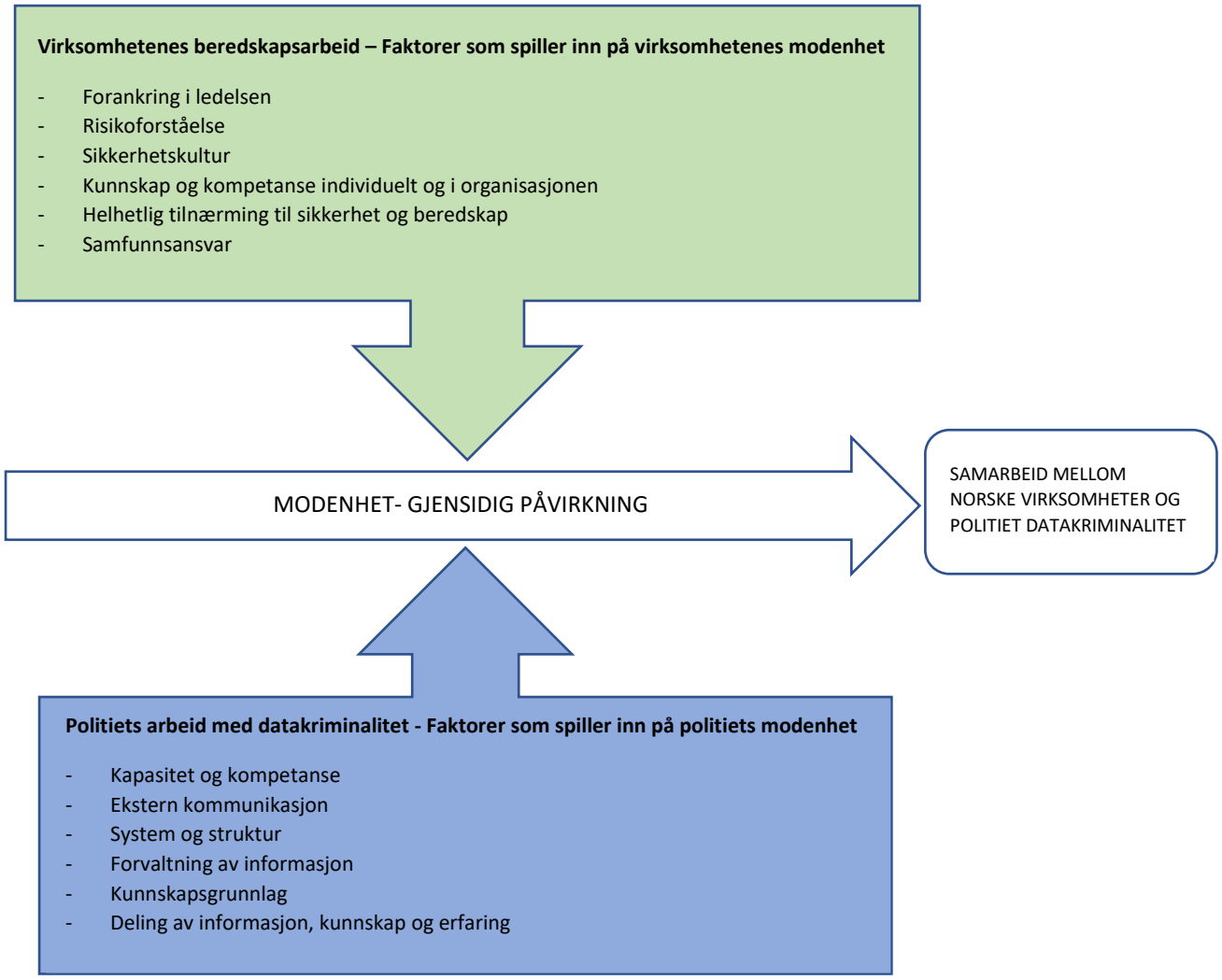
Flere av informantene tilknyttet politi- og lensmannsetaten fortalte at en viktig del av politiets forebyggende strategi når det kommer til datakriminalitet er å få i gang en «dugnad», altså å etablere holdninger og et tankesett hos virksomhetene om hva hensikten er med å dele informasjon om datakriminalitet med politiet. De forteller samtidig at det kan være utfordrende å motivere virksomhetene til å anmelde og dele informasjon når det er begrenset hva politiet kan gjøre med situasjonen de står i og det er usikkerhet rundt om politiet klarer å gi noe i retur. Informantene har sett eksempler på at virksomheter som både deler og som holder tilbake informasjon. I utvalg 1 er det forskjellige tanker og holdninger rundt dette, men flesteparten av informantene forteller at deres virksomhet er opptatt av samfunnsansvaret som

ligger i å dele informasjon om datakriminalitet. De ønsker å bidra til en større helhet og ser nytten i å dele og tenke langsiktig. Det er ikke sikkert at virksomhetene vil se en umiddelbar effekt dersom de velger å dele informasjon om for eksempel et dataangrep, men det handler om å se at informasjonen kan komme noen andre til gode. Og neste gang kan det kanskje være omvendt når noen andre deler. I utvalg 1 forteller flere av de opplever at situasjonen slik den har utviklet seg med trusselen fra datakriminelle og andre aktører som opererer i det digitale rom har gjort at alle må stå sammen. Likevel er det noen ganger de opplever utfordringer innad i egen virksomhet når det kommer til holdninger og tilnærminger til hvordan man håndterer informasjonen og hvem man involverer, eventuelt ikke involverer. Flere av informantene i utvalg 2 forteller at virksomhetenes forståelse av hva de kan bidra med når det kommer til forebygging og håndtering av datakriminalitet er viktig. Dette handler i stor grad handler om en aksept og forståelse for at selv om ikke politiet enda har den kompetansen og kapasiteten som kreves for å kunne gjøre en tilstrekkelig god jobb på dette området, noe som vil begrense hva virksomhetene kan få tilbake når de deler informasjon, må virksomhetene dele informasjon med politiet. I tillegg er det viktig at virksomhetene etablerer en holdning og kultur for å dele informasjon med en tanke om at informasjonen kanskje kan komme noen andre til gode.

> Dersom alle har denne holdningen og tilnærmingen vil virksomhetene kanskje en dag kunne nyttiggjøre seg av informasjonen som noen andre har kommet med. Neste gang kan det være noen andre som blir rammet og gangen etter der er det kanskje den samme virksomheten som blir rammet igjen. Vi ser jo det at når vi forfølger sporene eller den digitale infrastrukturen og havner på disse kommando-kontroll-serverne som gjerningspersonene bruker for å begå kriminaliteten, så ligger det ofte ferdig konfigurerte andre sluttmål inne på den serveren. Og det er ofte sluttmål som har blitt kompromittert, men ikke kryptert, så du har et handlingsvindu og et tidsvindu hvor vi kan varsle om et mulig kommende angrep i andre virksomheter. Da kan vi si at dere har noen på innsiden av systemene deres, men dere er ikke kryptert enda. Så hvis dere agerer nå så kan dere rekke å beskytte dere. Og når vi går gjennom de serverne finner norske virksomheter som har blitt kompromittert og kryptert, men som ikke har meldt dette til oss. Også kan vi sette opp en tidslinje, og hvis da den virksomheten hadde sagt ifra, så kunne vi kanskje ha advart den og den og den virksomheten unngått å bli rammet. Vi hadde kommet tidligere til den serveren og vi hadde blitt satt i stand til å

> advare andre. Og her kommer dette med dugnad inn (Ruben, Politi- og lensmannsetaten).

På samme måte som virksomhetene kan måles i modenhet, kan vi se politiets arbeid med datakriminalitet ses i rammen av modenhet. Dette vil i så fall dreie seg om hvor langt politiet har kommet i målsetningen som er satt for politiet i den nasjonale strategien, og hvorvidt samfunnet opplever at politiet evner å utføre sitt samfunnsoppdrag på en tilfredsstillende måte når det kommer til datakriminalitet (Departementene, 2019, s. 7). Sentrale elementer i politiets modenhet vil kunne være kapasitet, kompetanse, politiets eksterne kommunikasjon, system og struktur for forvaltning av informasjon fra publikum om datakriminalitet, etablering av kunnskapsgrunnlag og deling av informasjon, kunnskap og erfaring om datakriminalitet. Politiet slik det er i dag har ikke tilstrekkelig kompetanse og kapasitet til å forebygge og håndtere datakriminalitet på en tilfredsstillende måte (Riksrevisjonen, 2021). Gjennom intervjuene med begge intervjuutvalg har det kommet tydelig frem at det ikke står på viljen og ønsket, både hos norske virksomheter og politiet når det kommer til å samarbeide for å forebygge og håndtere datakriminalitet. Gjennom denne studien har det blitt tydelig at for å kunne møte truslene fra datakriminelle og fra det digitale rom må politiet og virksomhetene stå sammen, og virksomhetenes digitale beredskapsarbeid og politiets arbeid med datakriminalitet vil kunne ha en gjensidig påvirkning. Figur 5.3 illustrerer hvordan forskjellige faktorer hos de norske virksomhetene og politiet spiller inn på modenheten. De norske virksomhetene og politiet er avhengig av hverandres modenhet for å etablere et effektivt samarbeid når det kommer til forebygging og håndtering av datakriminalitet. De norske virksomhetene vil ha et behov for et politi som har kapasitet og kompetanse og som kan sette virksomhetene i stand til å beskytte seg selv gjennom å dele informasjon, kunnskap og erfaring om datakriminalitet som virksomhetene kan benytte inn i sitt beredskapsarbeid. I tillegg vil virksomhetene ha et behov for et politi som kan bistå dem i håndteringen av en krise dersom de blir utsatt for alvorlig datakriminalitet. For at politiet skal møte dette trenger politiet å etablere et kunnskapsgrunnlag om datakriminalitet, som igjen er avhengig av at de norske virksomhetene kan dele informasjon om datakriminalitet til politiet. Hvordan virksomhetene forholder seg til dette baserer seg på deres beredskapsarbeid, fokus på og forståelse av datakriminalitet som trussel, sikkerhetskulturen i virksomheten, en helhetlig tilnærming til sikkerhet og holdningene til samfunnsansvaret.



Figur 5.4 Samarbeid mellom de norske virksomhetene og politiet basert modenhet og gjensidig påvirkning

Dersom politiet deler informasjon og erfaring vil dette kunne øke kunnskapen og risikoforståelsen hos virksomhetene. Det kan tenkes at denne informasjonen også vil kunne bidra til at det digitale sikkerhetsarbeidet får større prioritet og fokus hos ledelsen og at dette igjen vil kunne etablere en bedre digital sikkerhetskultur hos virksomhetene. Et politi som aktivt tar eierskap til tematikken og kommuniserer godt med virksomhetene vil kunne motivere virksomhetene til å dele informasjon, både om mindre alvorlig og alvorlig datakriminalitet. Denne informasjonen vil kunne bidra til at politiet får et bedre kunnskapsgrunnlag som kan bidra til økte ressurser og bedre målretting av politiets arbeid.

5.5 Oppsummering analyse

Jeg har nå drøftet de empiriske funnene opp mot det teoretiske rammeverket i studien. I tillegg har jeg trukket inn aktuell internasjonal forskning og annen relevant litteratur som i hovedsak baserer seg på norske forhold og forebyggende sikkerhet- og beredskapsarbeid, samt politiets rolle når det kommer til forebygging og håndtering av datakriminalitet. Drøftingen har blitt satt i rammene av de fire hovedområdene bevissthet, beredskap, samvirke og modenhet inkluderer menneskelige og organisatoriske faktorer som har stor betydning for samarbeidet mellom virksomhetene og politiet. Hvordan de norske virksomhetene jobber med sikkerhet og beredskap, hvordan virksomhetens risikoforståelse er når det kommer til datakriminalitet og beredskapsarbeidets forankring i ledelsen har vist seg å være sentrale faktorer som spiller inn på hvordan virksomhetene forholder seg til et samarbeid med politiet når det kommer til datakriminalitet. På den andre siden spiller politiets arbeid med datakriminalitet inn på virksomhetenes beredskapsarbeid og samarbeid med politiet da dette legger grunnlaget for virksomhetenes tillit til politiet. Dette er også ett av de tre grunnleggende prinsippene for det offentlig-private samarbeidet; tillit, åpenhet og gjensidighet. Virksomhetenes og politiets modenhet i denne sammenheng handler om hvor langt virksomhetene og politiet har kommet i arbeidet med å etablere en effektiv forebygging og håndtering av trusselen som datakriminalitet utgjør, og modenheten hos begge parter vil ha en gjensidig påvirkning på hverandre.

6 Konklusjon

Truslene som datakriminalitet utgjør mot norske virksomheter i dag, øker i takt med digitaliseringen av samfunnet og de nye sårbarhetene som følger med. Fokuset på digital sikkerhet både fra myndighetene og blant norske virksomheter øker, og samarbeidet mellom virksomhetene og politiet når det kommer til datakriminalitet er dermed et svært aktuelt tema. Problemstillingen i denne studien var: «*Hvilke faktorer påvirker norske virksomheters samarbeid med politiet når det kommer til forebygging og håndtering av datakriminalitet?*».

For å svare på problemstillingen har jeg undersøkt hvordan samarbeidet oppleves av relevante personer i norske virksomheter og personer med tilknytning til politi- og lensmannsetaten, offentlige myndighetsorganer og i private sikkerhetsselskaper. Studien har gitt et innblikk i utfordringene knyttet til samarbeidet, og hvilke faktorer som kan påvirke samarbeidet positivt og negativt. Informantene som deltok i studien har bidratt med relevante erfaringer, opplevelser og informasjon om samarbeidet, som muliggjorde en inngående, sammensatt og dypere forståelse av temaet. Selv om dette forskningsprosjektet har gitt stor innsikt i hvilke faktorer som kan påvirke samarbeidet, vil det også kunne være andre faktorer som påvirker samarbeidet, som ikke har kommet frem gjennom studien.

Med bakgrunn i de empiriske funnene og kjerneelementene fra det teoretiske rammeverket, kom jeg frem til fire områder som belyser faktorer som kan ha stor betydning for samarbeidet mellom virksomhetene og politiet. Disse områdene utgjorde også de mest sentrale funnene i forskningsprosjektet:

- Bevissthet – risikoforståelse, ledelse og digital sikkerhetskultur
- Beredskapsarbeid – viktigheten av gode forberedelser
- Samvirke – Tillit, åpenhet og gjensidighet
- Modenhet – Helhetlig tilnærming til digital sikkerhet, samfunnsansvar og gjensidig avhengighet

De fire områdene dannet grunnlaget for analysen, hvor jeg drøftet empirien opp mot det teoretiske rammeverket, som i all hovedsak var kjente teorier innen samfunnssikkerhet og beredskap. Teoriene om menneskeskapte ulykker, organisatoriske ulykker og høypålitelige organisasjoner har bidratt med å sette tematikken inn i forskjellige sikkerhets- og beredskapsmessige perspektiver. I tillegg trakk jeg inn aktuell internasjonal forskning og annen relevant litteratur som i hovedsak baserer seg på norske forhold og forebyggende

sikkerhet- og beredskapsarbeid, samt politiets rolle når det kommer til forebygging og håndtering av datakriminalitet.

Studien har vist at faktorene som kan påvirke norske virksomheters samarbeid med politiet når det kommer til forebygging og håndtering av datakriminalitet i all hovedsak handler om menneskelige og organisatoriske faktorer knyttet til både de norske virksomhetene og politiet. Dette er faktorer som går på bevissthet, risikoforståelse, ledelse, sikkerhetskultur, og beredskapsarbeid. Resultatene fra studien belyser en varierende tilnærming til sikkerhets- og beredskapsarbeid i de norske virksomhetene når det kommer til digital sikkerhet og datakriminalitet. Videre viste studien stor intern variasjon og svakheter når det kommer til politiets arbeid med datakriminalitet, spesielt knyttet til kapasitet og kompetanse på området. Utfordringene knyttet til samarbeidet kan delvis begrunnes med at virksomhetene har manglende tillit til politiets håndtering av datakriminalitet, i tillegg til en usikkerhet knyttet til hva politiet kan bidra med, hvordan politiet jobber med datakriminalitet og politiets rolle i forbindelse med dette. Dette vil kunne påvirke hvorvidt virksomhetene inkluderer et samarbeid med politiet i arbeidet med sikkerhet- og beredskap, noe som gjennom studien har kommet frem som svært viktig. Dersom virksomhetene har gjort vurderinger knyttet til et samarbeid med politiet og implementert dette i beredskapsarbeidet før en hendelse inntreffer, vil sjansene kunne være større for at virksomhetene faktisk samarbeider med politiet dersom uhellet er ute. I denne forbindelse er det viktig at virksomhetene forstår hva politiet kan bidra med, hva slags informasjon politiet trenger og viktigheten av en tidlig involvering.

Samtidig som utfordringene i samarbeidet kan peke i retning av forhold ved politiets arbeid med datakriminalitet, er det også forhold ved virksomhetenes beredskapsarbeid som kan gjøre samarbeidet utfordrende. Hvordan virksomhetene forholder seg til datakriminalitet avhenger av virksomhetenes risikoforståelse når det kommer til trusselen som datakriminalitet utgjør, hvor godt forankret sikkerhets- og beredskapsarbeidet er i virksomhetens ledelse, hvordan sikkerhetskulturen i virksomheten er, hvilken kunnskap og kompetanse de ansatte og virksomheten som et kollektiv har når det kommer til digitale trusler og datakriminalitet, hvor helhetlig virksomheten jobber med beredskap og hvordan virksomheten forholder seg til et samarbeid med politiet basert på et ønske om å ta samfunnsansvar.

Gjennom forskningsprosjektet har begrepet modenhet gått igjen, både når det kommer til politiets arbeid med datakriminalitet og virksomhetenes beredskapsarbeid. Modenhet i denne sammenheng handler om hvor langt man har kommet mot målet om å få til en god og

effektiv forebygging og håndtering av datakriminalitet. Modenheten vil avhenge av forskjellige faktorer som danner en helhet, og inkluderer mange av faktorene som har vist seg å kunne være sentrale i samarbeidet. For politiet handler dette om hvordan datakriminalitet blir prioritert av politiledelsen og lokalt i politi-Norge. Dette vil kunne påvirke politiets kompetanse og kapasitet, og spiller inn på hvordan politiet etablerer sitt kunnskapsgrunnlag gjennom å forvalte den informasjonen som kommer inn fra norske virksomheter og andre aktører om datakriminalitet. Forebygging er politiets hovedstrategi, også når det kommer til datakriminalitet. Selv om politiet skal kunne straffeforfølge datakriminelle, vil det være viktig å sette norske virksomheter i stand til å beskytte seg mot trusselen som datakriminalitet utgjør gjennom det forebyggende arbeidet. For de norske virksomhetene handler modenhet om hvordan virksomhetene jobber med beredskap. Dette avhenger av at sikkerhets- og beredskapsarbeidet får allokert nok tid og ressurser gjennom forankring i ledelsen. Virksomhetens kollektive risikoforståelse er også sentralt i beredskapsarbeidet og avhenger av at virksomheten sitter på god informasjon om trusselen, egne verdier og sårbarheter. Kunnskap og kompetanse når det kommer til datakriminalitet vil sammen med god risikoforståelse og et helhetlig sikkerhets- og beredskapsarbeid, kunne etablere god sikkerhetskultur i virksomheten. Disse faktorene vil til sammen utgjøre virksomhetens modenhet, og vil kunne spille en sentral rolle i hvordan virksomhetene forholder seg til et samarbeid med politiet.

Et sentralt moment som har kommet frem gjennom forskningsprosjektet er at de norske virksomhetene og politiet vil kunne være gjensidig avhengig av hverandre når det kommer til forebygging og håndtering av datakriminalitet. Dette er også i tråd med offentlige dokumenter som sier noe om viktigheten av et offentlig-privat samarbeid i møtet med trusselen som datakriminalitet utgjør. Samarbeidet vil med det kunne avhenge av modenhet hos begge parter. Verken politiet eller virksomhetene kan møte trusselen som datakriminalitet utgjør alene, og både politiets og virksomhetenes modenhet vil med det kunne påvirke hverandre gjensidig. Dersom politiet prioriterer datakriminalitet og øker kapasitet og kompetanse gjennomgående i politiet, vil politiet kunne settes i stand til å både forebygge og håndtere datakriminalitet på en bedre måte. I dette ligger også å etablere et kunnskapsgrunnlag, som kan bidra til at politiet i større grad kan dele informasjon, kunnskap og erfaring med virksomhetene, som kan bruke denne informasjonen i sitt beredskapsarbeid. Dersom virksomhetene får til et godt beredskapsarbeid, vil dette kunne påvirke hvordan virksomhetene identifiserer og håndterer viktig informasjon og deler denne informasjon med

politiet, og involverer politiet dersom de blir utsatt for mindre alvorlig og alvorlig datakriminalitet. Den gjensidige påvirkningen, som baserer seg på en rekke faktorer knyttet til menneskelige og organisatoriske forhold, vil kunne påvirke samarbeidet mellom de norske virksomhetene og politiet når det kommer til forebygging og håndtering av datakriminalitet.

Tabell 6.1 viser en oversikt over koblingen mellom de fire mest sentrale funnene i oppgaven, kjerneelementer fra teorien, og implikasjoner knyttet til de norske virksomhetenes beredskapsarbeid og politiets arbeid med datakriminalitet basert på de empiriske funnene.

Hovedfunn	**Kjerneområder fra teorien**	**De norske virksomhetenes beredskapsarbeid - implikasjoner**	**Politiets arbeid med datakriminalitet - implikasjoner**
Bevissthet – risikoforståelse, ledelse og sikkerhetskultur	Risikoforståelse – noe subjektivt. Hvordan forstår man risiko? Sikkerhetskultur reflekterer ledelsens fokus på sikkerhet. Sikkerhetsarbeidet må forankres i ledelsen	Varierende hvordan virksomhetene forstår trusselen knyttet til datakriminalitet. Vanskelig å ha oversikt over et hurtig skiftende trusselbilde. Datakriminalitet mer abstrakt enn tradisjonell kriminalitet. Varierende hvordan lederne forstår g forholder seg til datakriminalitet. Dette spiller inn på allokeringen av tid og ressurser. Ledelsen må gå foran i arbeidet med å etablere sikkerhetskultur.	Manglende system for å forvalte informasjon fra virksomhetene på en god måte. Manglende kunnskapsgrunnlag og varierende kompetanse og kapasitet innad i politiet når det kommer til datakriminalitet. Satsing på næringslivskontakter vil kunne hjelpe med å dele informasjon, kunnskap og erfaring med virksomhetene.
Beredskap – viktigheten av gode forberedelser	Sikkerhet og beredskapsarbeid baserer seg på risikoforståelse og forankring i ledelsen. Unngå latente forhold, opprette forsvar i dybden gjennom harde og myke barrierer (f.eks. rutiner, prosedyrer, planer, trening og øving, kompetanseheving). Mindful organizing og sensemaking kan bidra til å forutse uønskede hendelser og unngå dem. Forpliktelse til resiliens og anerkjennelse av kompetanse vil hjelpe virksomheten med håndtering av situasjonen dersom uhellet er ute. Beredskapsarbeidets må foregå kontinuerlig og unngå symbolsk trygghet og fantasidokumenter. Operasjonalisering av tiltak.	Varierende hvordan virksomhetene jobber med beredskap og hvor godt forankret dette arbeidet er i ledelsen. Virksomhetene må operasjonalisere tiltakene fra beredskapsplanen. Dette vil kunne bidra til et godt samarbeid med politiet gjennom å gå opp kommunikasjonslinjer og forberede samarbeid.	Politiet opplever at virksomhetene jobber forskjellig med dette. erfaring med at de virksomhetene som har implementert kontakt med politiet i sine beredskapsplaner ofte har et bedre utgangspunkt for kontakt med politiet.
Samvirke – tillit, åpenhet og gjensidighet	Utfordringene knyttet til truslene fra det digitale rom og datakriminalitet utgjør krever et offentlig-privat samarbeid. Prinsippene som ligger til grunn for dette samarbeidet er tillit, åpenhet og gjensidighet.	Tilliten de norske virksomhetene har til politiets håndtering av datakriminalitet kan bli påvirket av politiets manglende kapasitet og kompetanse. Virksomhetenes åpenhet om datakriminalitet baserer seg på flere faktorer og vurderinger som gjøres i det enkelte tilfellet, som f.eks. omdømme, tid og prioriteringer, behov for kontroll på informasjon. Gjensidighet handler om deling av informasjon, kunnskap og erfaringer «begge veier». Virksomhetene vet ikke alltid hva de kan få igjen fra politiet og opplever ikke alltid at politiet	Politiet trenger informasjon fra virksomhetene for å etablere et godt kunnskapsgrunnlag. Politiets manglende kapasitet og kompetanse over tid når det kommer til datakriminalitet kan svekke tillitsforholdet. Politiet ønsker at virksomhetene skal være åpne og politiet får ikke gjort stort dersom ikke virksomhetene deler informasjon om hva de er utsatt for. Politiet har mye å gå på når det kommer til å kommunisere hva politiet trenger av informasjon, etablere systemer for god forvaltning av informasjonen og kommunisere hva politiet kan bidra med. Politiet kan ikke bistå virksomhetene i alle settinger hvor de har

		gir noe igjen. Dette baserer seg på kunnskap og erfaring. Det er et ønske fra virksomhetene om å etablere gode tillitsforhold, være åpne og bidra til gjensidighet.	blitt utsatt for alvorlig datakriminalitet, men kan basere andre avverginger/forebygging på informasjonen virksomheten kommer med. Politiet ønsker å kunne dele informasjon, kunnskap og erfaring for å bidra til virksomhetenes beredskapsarbeid.
Modenhet – helhetlig tilnærming til beredskapsarbeid og samfunnsansvar	Sikkerhets- og beredskapsarbeid krever en helhetlig tilnærming. Det må forankres i ledelsen og praktiseres gjennomgående i organisasjonen. Krever kontinuitet, oversikt, risikoforståelse, kunnskap og kompetanse. Sikkerhetstiltak må stå i stil til produksjon og må ikke bare få fokus etter at en uønsket hendelse har skjedd. For å måle hvordan en virksomhet ligger an med sikkerhets- og beredskapsarbeidet kan man se på modenhet, som er en helhet satt sammen av flere likeverdige deler knyttet til menneskelige, organisatoriske og teknologiske forhold. I samfunnsansvar ligger det å se at man er en del av noe større og at samfunnet vårt er satt sammen av avhengigheter.	Virksomhetenes modenhet kan måles i faktorer som ledelse, sikkerhetskultur, risikoforståelse, et kontinuerlig og helhetlig arbeid med beredskap. Det varierer mellom virksomhetene hvordan det står stilt med de forskjellige faktorene. Flere av virksomhetene har sett nytten av å jobbe helhetlig, og flere har sett at det ikke nytter å stå alene i møtet med trusselen som datakriminalitet utgjør. De ser at å dele informasjon om datakriminalitet med politiet vil kunne bidra til en større helhet, og at dette handler om en «dugnad» og holdninger. Likevel er det forskjell på hvordan dette fungerer i praksis. Virksomhetenes modenhet påvirkes av forhold i virksomheten, men virksomhetene ser også at politiets arbeid med datakriminaliteten kan spille dem gode i dette gjennom f.eks. å tilby informasjon som vil kunne bedre risikoforståelsen både hos ledelsen og i virksomheten som et kollektiv	Politiet ser på arbeidet med datakriminalitet som et «dugnadsarbeid» hvor både private og offentlige virksomheter må samarbeide og delta. Politiet ønsker å bistå med å sette virksomhetene i bedre stand til å beskytte seg selv gjennom deling av informasjon, kunnskap og erfaring. Det er viktig at virksomhetene tar samfunnsansvar og deler informasjon med politiet og involverer politiet tidlig. Politiets modenhet kan ses på i rammene av hvor langt politiet har kommet mtp. Mål som er satt fra myndighetene. Dette vil handle om kapasitet og kompetanse gjennomgående i politiet, og politiets evne til å både forebygge og håndtere datakriminalitet. Dette påvirkes også av det kunnskapsgrunnlaget politiet har, og avhenger med det bl.a. av informasjon fra virksomhetene.

Tabell 6.1 Kobling mellom hovedfunn, kjerneelementer fra teorien og implikasjoner knyttet til de norske virksomhetenes beredskapsarbeid og politiets arbeid med datakriminalitet

For fremtiden vil det være sentralt at både norske virksomheter og politiet etterlever prinsippene om tillit, åpenhet og gjensidighet for å spille hverandre gode i arbeidet med å forebygge og håndtere datakriminalitet. Et nøkkelord i denne sammenheng er god kommunikasjon. Virksomhetene må vite hvordan politiet jobber og hva slags informasjon politiet trenger, og politiet må dele informasjon om trusler og bidra i virksomhetenes digitale beredskapsarbeid. Det har blitt tydelig gjennom denne studien at det ikke står på ønske eller vilje hos noen av partene, det handler heller om faktorene knyttet til modenheten i møtet med datakriminalitet både hos de norske virksomhetene og politiet, som vil ha en gjensidig påvirkning på hverandre, og dermed en direkte påvirkning på samarbeidet.

6.1 Videre forskning

Forskningsprosjektet har jeg snakket med personer ansatt i store norske virksomheter. De representerte med det virksomheter hvor det kan forventes tydelig struktur og organisering, samt god tilgang på ressurser, sammenlignet med små og mellomstore virksomheter. I tillegg snakket jeg med personer som jobber med digital sikkerhet i politi- og lensmannsetaten, et

offentlig myndighetsorgan og private sikkerhetsselskaper som jobber med datakriminalitet. Det kunne vært interessant som en videreføring av prosjektet å utvide dette til å intervjue personer fra små og/eller mellomstore virksomheter da det vil kunne være variasjoner i hvilke faktorer som spiller inn på deres samarbeid med politiet, og eventuelt se på om politiet må tilnærme seg disse virksomhetene på en annen måte i det forebyggende arbeidet. Her kunne man ha sammenlignet resultatene med det som har kommet frem i denne studien for å se om det er andre faktorer som vil spille inn på samarbeidet i den settingen. I tillegg kunne det ha vært av interesse å intervjue polititjenestepersoner som jobber med datakriminalitet i flere forskjellige politidistrikt og sett på hva som påvirker politiets interne forskjeller i arbeidet med datakriminalitet, samt gjort en kartlegging av hva politiet gjør aktivt for å bedre både kapasitet og kompetanse.

Referanser

Aakre, S. (2020). Hvilket trusselbilde står norske virksomheter overfor, og hvordan kan åpenhet bidra til å forstå cyberrisiko? *Magma (0220), s. 37-45.*

Aven, T. & Renn, O. (2010). *Risk Management and Governance.* (1. utg.). Berlin: Springer-Verlag.

Aven, T., Boyesen, M., Njå, O., Olsen, K. H., & Sandve, K. (2019). *Samfunnssikkerhet.* (9. utg.). Oslo: Universitetsforlaget.

Bergsjø, H. & Windvik, R. (2018). *Datasikkerhet for ledere – hvordan beskytte din virksomhet.* (1. utg.). Oslo: Universitetsforlaget

Bergsjø, H., Windvik, R. & Øverlier, Ø. (2020). *Digital sikkerhet – en innføring.* Oslo: Universitetsforlaget

Blaikie, N. (2010). *Designing Social Research.* (2. utg.). Cambridge: Polity

Departementene. (2019). *Nasjonal strategi for digital sikkerhet.* Justis- og beredskapsdepartementet og Forsvarsdepartementet. Hentet fra nasjonal-strategi-for-digital-sikkerhet.pdf (regjeringen.no)

Direktoratet for samfunnssikkerhet og beredskap (DSB) (2016). *Samfunnskritiske funksjoner – hvilken funksjonsevne må samfunnet opprettholde til enhver tid.* Hentet fra kiks-2_januar.pdf (dsb.no)

Engen, O. A. H., Pettersen Gould, K. A., Kruke, B. I., Hempel Lindøe, P., Olsen, K. H. & Olsen, O. E. (2021). *Perspektiver på samfunnssikkerhet.* (2. utg.). Oslo: Cappelen Damm Akademisk

Europol (2017). *Internet Organised Crime Threat Assessment 2017.* Hentet fra iocta2017.pdf (europa.eu)

Europol (2021). *Internet Organised Crime Threat Assessment 2021.* Hentet fra internet_organised_crime_threat_assessment_iocta_2021.pdf (europa.eu)

Hadnagy, C. (2018). *Social Engineering – The Science of Human Hacking.* (2. Utg.). Wiley

Johannessen, A., Christoffersen, L. & Tufte, P. A. (2020). *Forskningsmetode for økonomisk-administrative fag.* (4. utg.). Oslo: Abstrakt forlag

Justis- og beredskapsdepartementet. (2015). *Justis og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet.* Hentet fra Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet (regjeringen.no)

Jøsang, A. (2021). *Informasjonssikkerhet – Teori og praksis.* (1. utg.). Oslo: Universitetsforlaget

Kemp, S., Buil-Gil, D., Miró-Llinares, F. & Lord, N. (2021). When do businesses report cybercrime? Findings from a UK study. *Criminology & Criminal Justice.* I-22. https://doi.org/10.1177/17488958211062359

Knight, R. F. & Pretty, D. J. (2001). *Reputation and value – the case of corporate catastrophes.* Oxford Metrica. Hentet fra 01RepComAIG.pdf (oxfordmetrica.com)

KPMG (2016, 25, mai). *Ta den viktige helsesjekken!* Ta den viktige helsesjekken! - KPMG Norge (home.kpmg)

Lunde, I. K. (2019). *Praktisk krise- og beredskapsledelse.* (2. utg.). Oslo: Universitetsforlaget.

Meld. St. 17 (2001-2002). *Samfunnssikkerhet – Veien til et mindre sårbart samfunn..* Justis- og beredskapsdepartementet. Hentet fra STM017000-A.fm (regjeringen.no)

Meld. St. 38 (2016-2017). *IKT-sikkerhet – Et felles ansvar.* Justis- og beredskapsdepartementet. Hentet fra Meld. St. 38 (2016–2017) (regjeringen.no)

Meld. St. 29 (2019-2020). *Politimeldingen – et politi for fremtiden.* Justis- og beredskapsdepartementet. Hentet fra Meld. St. 29 (2019–2020) (regjeringen.no)

Nilssen, V. (2012). *Analyse i kvalitative studier – Den skrivende forskeren.* (1. utg.). Oslo: Universitetsforlaget

Nasjonal sikkerhetsmyndighet (NSM) (2017). *Risiko 2017 – Risiko og sårbarheter i en ny tid.* Hentet fra nsm_risiko_2017_lr_0404_enkelts_v3.pdf

Nasjonal sikkerhetsmyndighet (NSM) (2019). *Helhetlig digitalt risikobilde 2019.* Hentet fra 2019---nsm-helhetlig-digitalt-risikobilde.pdf

Nasjonal sikkerhetsmyndighet (NSM) (2020). *Helhetlig digitalt risikobilde 2020.* Hentet fra NSM_IKT-risikobilde_2020_enkeltside.pdf

Nasjonal sikkerhetsmyndighet (NSM) (2021). *Nasjonalt digitalt risikobilde 2021.* Hentet fra Nasjonalt digitalt risikobilde 2021 - Nasjonal sikkerhetsmyndighet (nsm.no)

Nasjonal sikkerhetsmyndighet (NSM) (u.å). *Nasjonalt cybersikkerhetssenter (NCSC).* Hentet 20. mars 2022 fra Nasjonalt cybersikkerhetssenter - Nasjonal sikkerhetsmyndighet (nsm.no)

Nätt, T. H. & Heide, C. F. (2019). *Datasikkerhet – ikke bli svindlerens neste offer.* (2. utg.). Oslo: Gyldendal

National Cyber Security Centre (NCSC) (2018, 8. mars). *Maturity models in cyber security: what's happening to the IAMM?* Maturity models in cyber security: what's happening to the... - NCSC.GOV.UK

Norsk senter for informasjonssikring (NorSIS) (2016). *The Norwegian Cyber Security Culture.* Hentet fra The-Norwegian-Cybersecurity-culture-web.pdf (norsis.no)

NOU 2000:24. (2000). *Et sårbart samfunn – Utfordringene for sikkerhets og beredskapsarbeidet i samfunnet.* Justis- og beredskapsdepartementet. NOU 2000: 24 - regjeringen.no

Næringslivets sikkerhetsråd (NSR) (2019). *Hybridundersøkelsen – Hybride trusler og hendelser mot norsk næringsliv.* Hentet fra Hybridundersokelsen-2019 (2).pdf

Næringslivets sikkerhetsråd (NSR) (2020). *Mørketallsundersøkelsen 2020.* Hentet fra Morketalls-2020-web (7).pdf

Næringslivets sikkerhetsråd (NSR) (2021, 13. oktober). *Viktig fokus på digital kriminalitet og beredskap i Hurdalsplattformen.* Hentet fra Viktig fokus på digital kriminalitet og beredskap i Hurdalsplattformen – Næringslivets Sikkerhetsråd (nsr-org.no)

Olsen, O. E. & Mathiesen, E. R. (2019). *Media og krisehåndtering – Utfordringer i en ny mediehverdag.* (2. utg.). Oslo: Cappelen Damm Akademisk

Oslo politidistrikt (2018). *Trender i kriminalitet 2018-2021: Digitale og lokale utfordringer.* Hentet fra Epubl3 utgave Trendrapport opd 2018 (politiet.no)

Politidirektoratet (POD) (2017). *Trusler og utfordringer innen IKT-kriminalitet (2017).* Hentet fra ikt_krim_pod.pdf (politiet.no)

Politidirektoratet (POD) (2020). *I forkant av kriminaliteten – Forebygging som politiets hovedstrategi (2021-2025).* Hentet fra i-forkant-av-kriminaliteten.pdf (politiet.no)

Politidirektoratet (POD) (2021). *Politiets trusselvurdering 2021.* Hentet fra 2021-02-12-o-ptv-2021.pdf (politiet.no)

Politiet. (u.å.). *Nasjonalt cyberkrimsenter (NC3).* Hentet 20. mars 2022 fra Nasjonalt cyberkrimsenter – Politiet.no

Reason, J. (1997). *Managing the Risks of Organizational Accidents.* Aldershot: Ashgate

Reliable & Secure Information (RSI Security) (2020, 21. August). *Does your Company need Cyber Maturity Assessment?* Does Your Company Need Cyber Maturity Assessment? | RSI Security

Renn, O. (2008). *Risk Governance – Coping with Uncertainty in a Complex World.* (1. Utg.). London og New York: Earthscan

Riksrevisjonen (2021). *Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT.* Hentet fra Dokument 3:5 (2020-2021) (riksrevisjonen.no)

Thon, R. (2020, 5. August). *Bedriftene må være åpne om dataangrep.* Nasjonal sikkerhetsmyndighet. Bedriftene må være åpne om dataangrep - Nasjonal sikkerhetsmyndighet (nsm.no)

Tjora, A. (2012). *Kvalitative forskningsmetoder i praksis.* (2. utg.). Oslo: Gyldendal Akademisk

Turner, B. A. (1978). *Man-Made disasters.* (1. utg.). London: Wykeham Science Press.

Van de Weijer, S., Leukfeldt, R. & Van der Zee, S. (2019). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal Vol. 43 No. 1, 2020 pp. 17-34.* https://doi.org/10.1108/PIJPSM-07-2019-0122

Weick, K. E. & Sutcliffe, K. M. (2015). *Managing the unexpected – Sustained Performance in a Complex World.* (3. Utg.). Hoboken, New Jersey: Wiley

Wanamaker, K. A. (2019). *Profile of Canadian Businesses who Report Cybercrime to Police: The 2017 Canadian Survey of Cyber Security and Cybercrime.* Research report: 2019-

R006. Hentet fra 2021-12-28_Profile of canadian businesses wh port cybecrime to police.pdf

Økokrim. (u.å). *Bedrageri*. Hentet 20. mars 2022 fra Bedrageri - Økokrim (okokrim.no)

Vedlegg

Vedlegg 1 – Informasjonsskriv og samtykkeskjema utvalg 1

Vil du stille til intervju i forskningsprosjektet

Hvilke faktorer påvirker norske virksomheters samarbeid med politiet når det kommer til forebygging og håndtering av datakriminalitet?

Dette er en forespørsel til deg om å delta i et forskningsprosjekt i forbindelse med en masterstudie ved Nord universitet *Erfaringsbasert master i beredskap og kriseledelse*. Dette skrivet vil gi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg og din arbeidsplass, hvordan dine personopplysning vil bli behandlet og hvilke rettigheter du har.

Formål

Prosjektet søker å belyse hvilke faktorer som spiller inn på samarbeidet mellom norske virksomheter og politiet i forbindelse med forebygging og håndtering av datakriminalitet. Hensikten er å få bedre forståelse for bakenforliggende årsaker til hva som hemmer eller fremmer et samarbeidet. Informasjon om og bedre forståelse for dette kan bidra til å identifisere tiltak som kan være med på å styrke et samarbeid, bygge kompetanse og forbedre det forebyggende arbeidet mot datakriminalitet.

Hvem er ansvarlig for forskningsprosjektet?

Ansvarlig for prosjektet er Nord universitet.
Veileder: Per Arne Godejord
Student: Benedicte Bjartland

Hvorfor får du spørsmål om å delta?

Metoden som er valgt for studien er personintervju. For å få relevant informasjon som vil kunne bidra til å besvare problemstillingen og forskningsspørsmålene er det ønskelig å intervjue personer i norske virksomheter som har en sentral rolle i arbeidet med digital beredskap, forebygging og håndtering av datakriminalitet, og som er med på å vurdere om virksomheten deler informasjon, er åpen og involverer politiet i forbindelse med mindre alvorlig og alvorlig datakriminalitet.

Forespørselen vil sendes til flere norske virksomheter. Å intervjue personer i forskjellige norske virksomheter som er sentrale i virksomhetens sikkerhets- og beredskapsarbeid vil kunne bidra til et bredt datagrunnlag som vil være viktig nå det kommer til å identifisere faktorer som kan bidra til et bedre samarbeid mellom politiet og virksomhetene i forbindelse med datakriminalitet.

Hva innebærer det for deg å delta?

Det vil settes av inntil 1 time til intervjuet. Hvor mye av den tiden som benyttes avhenger av informasjonen som kommer frem. Intervjuene tas opp på lyd og vil transkriberes i etterkant av selve intervjuet. Det er ønskelig at intervjuet gjennomføres i løpet av januar 2022.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Både arbeidsplass og intervjuobjekt vil anonymiseres. Opplysningene om intervjuobjekter og deres ansettelsessted skal derfor ikke benyttes til andre formål enn til å skille mellom de forskjellige intervjuobjektene. Opplysningene som kommer frem under intervjuene, både personopplysninger og informasjonen som ønskes innhentet, vil ikke kunne spores tilbake til person eller arbeidsgiver i selve masteroppgaven.

Opplysningene om deg vil kun brukes til formålene som er omhandlet i dette skrivet. Opplysningene vil bli behandlet konfidensielt og i samsvar med personvernregelverket.

Personopplysningene som er viktige i forbindelse med intervjuene er navn, stilling, arbeidsgiver og telefonnummer og eller/epostadresse. Disse opplysningene vil ikke komme frem i oppgaven, men vil lagres for å kunne skille de forskjellige intervjuene fra hverandre.

Behandlingsansvarlig institusjon er Nord universitet. Det er veileder Per Arne Godejord og student Benedicte Bjartland som, i tillegg til behandlingsansvarlig institusjon, vil ha tilgang til opp opplysningene.

Tiltak som iverksettes for å sikre at ingen uvedkommende får tilgang til personopplysningene:

Personopplysningene til intervjuobjektene, navn, arbeidsgiver, stilling og telefonnummer og epostadresse vil noteres i et dokument som ligger på en ekstern passord-beskyttet lagringsenhet. Hvert intervjuobjekt vil få tildelt en unik identitet/kode som lagres på en egen navneliste adskilt fra øvrige data. Under arbeidsfasen og analysen av data og utforming av masteroppgaven vil denne unike identiteten (f.eks. IO1U1) benyttes i stedet for navn. Det samme gjelder arbeidssted. Ved ferdigstillelse av oppgaven vil unik identitet også fjernes fra oppgaveteksten. Der det er ønskelig å referere til et intervjuobjekt eller benytte utdrag fra intervjuet vil et pseudonym brukes i stedet for intervjuobjektets navn. Alle intervjuobjektene vil tildeles et pseudonym og arbeidsplassen vil omtales under en bransjekategori, f.eks. «Industri». Det vil ikke fremkomme informasjon som kan knytte dette til person. Lydfilene fra intervjuene vil bli lagret på en ekstern lagringsenhet uten tilkobling for internett, i tillegg til Nord universitet sin applikasjon for laging av lydfiler (Nettskjema diktafon) som er godkjent av NSD for bruk i forskningsprosjekter.

Deltakerne i prosjektet vil ikke kunne gjenkjennes i publikasjonen. Opplysningene som vil publiseres er resultatene fra dataanalysen, altså sammenstillingen og funn gjort under undersøkelsen. Det vil ikke komme frem informasjon i publikasjonen om hvilke virksomheter eller offentlige bedrifter som har bidratt med intervjuobjekter til prosjektet, og det vil ikke settes søkelys på det enkelte intervjuobjektets bidrag, men bidragene som helhet.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er i mai 2022. Det er ikke behov for å oppbevare eller ha tilgang til opplysningene og lydopptak ved prosjektslutt, og informasjonen vil dermed slettes.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene
- å få rettet personopplysninger om deg
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Nord universitet har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?

Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Nord universitet ved prosjektansvarlig Per Arne Godejord.
  E-post: per.a.godejord@nord.no
- Student Benedicte Bjartland
  E-post: 332107@nord.no
- Vårt personvernombud Toril Irene Kringen
  Tlf.: 74 02 27 50
  E-post: personvernombud@nord.no

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Prosjektansvarlig	*Student*
Per Arne Godejord	Benedicte Bjartland

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Hvilke faktorer påvirker norske virksomheters samarbeid med politiet når det kommer til forebygging og håndtering av datakriminalitet?*

og har fått anledning til å stille spørsmål. Jeg samtykker til:

☐ å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet-

---

(Signert av prosjektdeltaker , dato)

Vedlegg 2 – Informasjonsskriv og samtykkeskjema utvalg 2

Vil du stille til intervju i forskningsprosjektet

Hvilke faktorer påvirker norske virksomheters samarbeid med politiet når det kommer til forebygging og håndtering av datakriminalitet?

Dette er en forespørsel til deg om å delta i et forskningsprosjekt i forbindelse med en masterstudie ved Nord universitet *Erfaringsbasert master i beredskap og kriseledelse*. Dette skrivet vil gi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg og din arbeidsplass, hvordan dine personopplysning vil bli behandlet og hvilke rettigheter du har.

Formål

Prosjektet søker å belyse hvilke faktorer som spiller inn på samarbeidet mellom norske virksomheter og politiet i forbindelse med forebygging og håndtering av datakriminalitet. Hensikten er å få bedre forståelse for bakenforliggende årsaker til hva som hemmer eller fremmer et samarbeidet. Informasjon om og bedre forståelse for dette kan bidra til å identifisere tiltak som kan være med på å styrke et samarbeid, bygge kompetanse og forbedre det forebyggende arbeidet mot datakriminalitet.

Hvem er ansvarlig for forskningsprosjektet?

Ansvarlig for prosjektet er Nord universitet.
Veileder: Per Arne Godejord
Student: Benedicte Bjartland

Hvorfor får du spørsmål om å delta?

Metoden som er valgt for studien er personintervju. Det har blitt sendt ut forespørsel om intervju til ansatte i flere norske virksomheter som har en sentral rolle i virksomhetens sikkerhets- og beredskapsarbeid, og som er sentrale i vurderingene rundt samarbeid med myndigheter og politiet når det kommer til utfordringene knyttet til datakriminalitet. I tillegg til å intervjue personer ansatt i norske virksomheter er det ønskelig å intervjue personer med en særskilt kompetanse, erfaring, rolle, stilling og/eller oppdatert kunnskap om tematikken for å belyse temaet ytterligere. Med bakgrunn i dette blir du spurt om å delta i studien.

Hva innebærer det for deg å delta?

Det vil settes av inntil 1 time intervjuet. Hvor mye av den tiden som benyttes avhenger av informasjonen som kommer frem. Intervjuene tas opp på lyd og vil transkriberes i etterkant av selve intervjuet. Det er ønskelig at intervjuet gjennomføres før utgangen av 2021, eller i løpet av januar 2022.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Både arbeidsplass og intervjuobjekt vil anonymiseres. Opplysningene om intervjuobjekter og deres ansettelsessted skal derfor ikke benyttes til andre formål enn til å skille mellom de forskjellige intervjuobjektene. Opplysningene som kommer frem under intervjuene, både personopplysninger og informasjonen som ønskes innhentet, vil ikke kunne spores tilbake til person eller arbeidsgiver i selve masteroppgaven.

Opplysningene om deg vil kun brukes til formålene som er omhandlet i dette skrivet. Opplysningene vil bli behandlet konfidensielt og i samsvar med personvernregelverket.

Personopplysningene som er viktige i forbindelse med intervjuene er navn, stilling, arbeidsgiver og telefonnummer og/eller epostadresse. Disse opplysningene vil ikke komme frem i oppgaven, men vil lagres for å kunne skille de forskjellige intervjuene fra hverandre og for å avtale tid og sted for intervju.

Behandlingsansvarlig institusjon er Nord universitet. Det er veileder Per Arne Godejord og student Benedicte Bjartland som, i tillegg til behandlingsansvarlig institusjon, vil ha tilgang til opp opplysningene.

Tiltak som iverksettes for å sikre at ingen uvedkommende får tilgang til personopplysningene:

Personopplysningene til intervjuobjektene, navn, arbeidsgiver, stilling og telefonnummer og epostadresse vil noteres i et dokument som ligger på en ekstern passord-beskyttet lagringsenhet. Hvert intervjuobjekt vil få tildelt en unik identitet/kode som lagres på en egen navneliste adskilt fra øvrige data. Under arbeidsfasen og analysen av data og utforming av masteroppgaven vil denne unike identiteten (f.eks. IO1U1) benyttes i stedet for navn. Det samme gjelder arbeidssted. Ved ferdigstillelse av oppgaven vil unik identitet også fjernes fra oppgaveteksten. Der det er ønskelig å referere til et intervjuobjekt eller benytte utdrag fra intervjuet vil et pseudonym brukes i stedet for intervjuobjektets navn. Alle intervjuobjektene vil tildeles et pseudonym og arbeidsplassen vil omtales under en bransjekategori, f.eks. «Industri». Det vil ikke fremkomme informasjon som kan knytte dette til person. Lydfilene fra intervjuene vil bli lagret på en ekstern lagringsenhet uten tilkobling for internett, i tillegg til Nord universitet sin applikasjon for laging av lydfiler (Nettskjema diktafon) som er godkjent av NSD for bruk i forskningsprosjekter.

Deltakerne i prosjektet vil ikke kunne gjenkjennes i publikasjonen. Opplysningene som vil publiseres er resultatene fra dataanalysen, altså sammenstillingen og funn gjort under

undersøkelsen. Det vil ikke komme frem informasjon i publikasjonen om hvilke virksomheter eller offentlige bedrifter som har bidratt med intervjuobjekter til prosjektet, og det vil ikke settes søkelys på det enkelte intervjuobjektets bidrag, men bidragene som helhet.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er i mai 2022. Det er ikke behov for å oppbevare eller ha tilgang til opplysningene og lydopptak ved prosjektslutt, og informasjonen vil dermed slettes.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene
- å få rettet personopplysninger om deg
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Nord universitet har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?

Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Nord universitet ved prosjektansvarlig Per Arne Godejord.
  E-post: per.a.godejord@nord.no
- Student Benedicte Bjartland
  E-post: 332107@nord.no
- Vårt personvernombud Toril Irene Kringen
  Tlf.: 74 02 27 50
  E-post: personvernombud@nord.no

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Prosjektansvarlig	*Student*
Per Arne Godejord	Benedicte Bjartland

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Hvilke faktorer påvirker norske virksomheters samarbeid med politiet når det kommer til forebygging og håndtering av datakriminalitet?*

og har fått anledning til å stille spørsmål. Jeg samtykker til:

☐ å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av , dato)

Vedlegg 3 – Godkjenning fra NSD

NSD sin vurdering

Referansenummer
711798

Prosjekttittel
Masteroppgave Beredskap og kriseledelse

Behandlingsansvarlig institusjon
Nord Universitet / Handelshøgskolen / Marked, organisasjon og ledelse

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)
Per Arne Godejord, per.a.godejord@nord.no, tlf.: 75517000

Type prosjekt
Studentprosjekt, masterstudium

Kontaktinformasjon, student
Benedicte Bjartland, 332107@student.nord.no

Prosjektperiode
20.08.2021 - 31.05.2022

Vurdering (1)

19.11.2021 - Vurdert

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg den 19.11.2021, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 31.05.2022

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om: · lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen · formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles til nye, uforenlige formål · dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet · lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet.

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), og dataportabilitet (art. 20). NSD vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13. Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32). Ved bruk av databehandler (spørreskjemaleverandør, skylagring eller videosamtale) må behandlingen oppfylle kravene til bruk av databehandler, jf. art 28 og 29. Bruk leverandører som din institusjon har avtale med. For å forsikre dere om at kravene

oppfylles, må dere følge interne retningslinjer og/eller rådføre dere med behandlingsansvarlig institusjon.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde: https://www.nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/melde-endringer-i-meldeskjema Du må vente på svar fra NSD før endringen gjennomføres.

OPPFØLGING AV PROSJEKTET
NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet. Lykke til med prosjektet!

Vedlegg 4 – Intervjuguide utvalg 1

Intervjuguide utvalg 1

Innledning:

- Informasjon om meg: utdanningsbakgrunn, nåværende jobb, interesser og hva som ledet til valg av tema for masteroppgaven
- Informasjon om prosjektet: hvorfor intervjuobjektet har blitt spurt om å delta, hva studien går ut på, de forskjellige intervjuutvalgene, formål
- Informasjon om innhenting av personopplysninger: sjekke at intervjuobjektet har fått lest gjennom og forstått informasjonen i informasjonsskrivet, bruk av lydopptak, samtykke og eventuelle spørsmål intervjuobjektet ønsker å stille før intervjuet begynner
- Informasjon om intervjuets oppbygging: tema, ønske om at intervjuobjektet skal fortelle så mye som mulig og snakke fritt, spørsmål, avslutning og tidsbruk

Oppvarmingsspørsmål:

- Kan du fortelle litt om din bakgrunn, hvor du er ansatt nå og hvilken rolle du har?
- Kan du fortelle meg hva slags forhold til og/eller erfaring du har når det kommer til håndtering og forebygging av uønskede digitale hendelser/datakriminalitet?

Refleksjonsspørsmål – faktorer som påvirker samarbeidet virksomheter/politi:

Informer om at det mest sentrale spørsmålet i intervjuet kommer tidlig fordi jeg ønsker at intervjuobjektet snakker fritt om det før vi har snakket om det og intervjuobjektet blir påvirket av spørsmål og av mine tanker og oppfatninger om temaet.

- Hvilke faktorer mener du at påvirker din virksomhets samarbeid med politiet når det kommer til å forebygge og håndtere datakriminalitet?

Her ønsker jeg å høre om faktorer som både kan hemme og fremme et godt samarbeid, og du kan gjerne trekke frem konkrete eksempler og fortelle om dine erfaringer.

- Hva mener du er viktig for norske virksomheter når det kommer til god og helhetlig håndtering av datakriminalitet/datasikkerhetshendelser?
- Hvordan jobber din virksomhet med digital beredskap?
- I hvilken grad vil du si at din virksomhet er forberedt på alvorlig datakriminalitet som for eksempel et dataangrep?
- Er myndighetskontakt/kontakt med politiet noe din virksomhet har tatt stilling til når det kommer til datakriminalitet?
- Hvordan stiller ledelsen i din virksomhet seg til samarbeid med politiet?
- Har din virksomhet erfaring fra samarbeid med politiet når det kommer til datakriminalitet?

Stikkord: Kost/nytte, egeninteresse, tid, prioriteringer, omdømme, samfunnsansvar, kunnskap, kompetanse, politiets arbeid med datakriminalitet, tilgjengelighet, enkelhet, beredskapsarbeid, beredskapsplaner, strategi, ledelse, tredjeparts påvirkning, alvorlighetsgrad datakriminalitet.

Samfunnsansvar:

- Hvor står din virksomhet når det kommer til tanken om å dele informasjon med politiet, både når det gjelder mindre alvorlige og alvorlige hendelser, for å forebygge datakriminalitet?
- Har din virksomhet har et bevisst forhold til politiets rolle når det kommer til datakriminalitet?
- Hvilken forskjell tror du det vil utgjøre dersom din virksomhet, og andre virksomheter, velger å dele informasjon og involvere politiet i forbindelse med datakriminalitet?

Tanker om samarbeid og forventninger til politiets arbeid med datakriminalitet:

- Har din virksomhet erfaring fra samarbeid med politiet når det kommer til datakriminalitet?
- Har du noen tanker om hva politiet kan gjøre for å legge bedre til rette for samarbeid med din virksomhet og andre norske virksomheter i forbindelse med håndtering og forebygging av datakriminalitet?
- Har du og din virksomhet merket noen forskjell i politiets forebyggende arbeid med datakriminalitet de siste årene?
- Når det kommer til å forebygge og håndtere datakriminalitet, hvilke forventninger har din virksomhet til politiet på dette området for fremtiden?
- Dersom din virksomhet skal samarbeide med politiet i forbindelse med datakriminalitet, hva er viktig for din virksomhet i dette samarbeidet?

Avslutningsspørsmål:

- Ut fra det vi har snakket om, er det anen informasjon, andre synspunkter eller noe du ønsker å tilføye?
- Har du noen avsluttende tanker om forskningsprosjektet som du ønsker å dele?
- Er det i orden om jeg kontakter deg igjen dersom jeg har oppfølgingsspørsmål eller behov for å oppklare noe?

Vedlegg 5 – Intervjuguide utvalg 2

Intervjuguide utvalg 2

Innledning:

- Informasjon om meg: utdanningsbakgrunn, nåværende jobb, interesser og hva som ledet til valg av tema for masteroppgaven
- Informasjon om prosjektet: hvorfor intervjuobjektet har blitt spurt om å delta, hva studien går ut på, de forskjellige intervjuutvalgene, formål
- Informasjon om innhenting av personopplysninger: sjekke at intervjuobjektet har fått lest gjennom og forstått informasjonen i informasjonsskrivet, bruk av lydopptak, samtykke og eventuelle spørsmål intervjuobjektet ønsker å stille før intervjuet starter
- Informasjon om intervjuets oppbygging: tema, ønske om at intervjuobjektet skal fortelle så mye som mulig og snakke fritt, spørsmål, avslutning og tidsbruk

Oppvarmingsspørsmål:

- Kan du fortelle litt om din bakgrunn, hvor du er ansatt nå og hvilken rolle du har?
- Kan du fortelle meg hva slags forhold til og/eller erfaring du har når det kommer til håndtering og forebygging av datakriminalitet?

Refleksjonsspørsmål:

Informer om at det mest sentrale spørsmålet i intervjuet kommer tidlig fordi jeg ønsker at intervjuobjektet snakker fritt om det før vi har snakket om det og intervjuobjektet blir påvirket av spørsmål og av mine tanker og oppfatninger om temaet.

- Hvilke faktorer mener du at påvirker norske virksomhets samarbeid med politiet når det kommer til å forebygge og håndtere datakriminalitet?

Stikkord: Kost/nytte, egeninteresse, tid, prioriteringer, omdømme, samfunnsansvar, kunnskap, kompetanse, politiets arbeid med datakriminalitet, tilgjengelighet, enkelhet, beredskapsarbeid, beredskapsplaner, strategi, ledelse, tredjeparts påvirkning, alvorlighetsgrad datakriminalitet.

Politiets arbeid med datakriminalitet og samarbeid med norske virksomheter

- Kan du fortelle om det du kjenner til av politiets forebyggende strategi og hva politiet trenger for å kunne drive forebygging og håndtering av datakriminalitet rettet mot norske virksomheter?
- Tror du at norske virksomheter har et bevisst forhold til hva datakriminalitet er og hva politiets rolle er når det kommer til datakriminalitet?
- Hvordan kan politiet legge til rette for et godt samarbeid med norske virksomheter når det kommer til forebygging og håndtering av datakriminalitet?
- Hvilke utfordringer tenker du at norsk politi har når det kommer til arbeidet med datakriminalitet?
- Hvilken innvirkning kan det ha på politiets arbeid dersom virksomheter ikke er åpne og deler informasjon med politiet om datakriminalitet?
- Hva tenker du at politiet kan bidra med for å hjelpe norske virksomheter i arbeidet med digital beredskap?

- Hva mener du at er viktig at politiet bidrar med til norske virksomheter når de er utsatt for mindre alvorlig og alvorlig datakriminalitet?
- Hva tenker du om politiets eksterne kommuniserer til norske virksomheter når det kommer til hva virksomhetene kan forvente av politiet, hva politiet kan bidra med, hva slags informasjon politiet trenger at virksomhetene deler og hvordan politiet jobber med datakriminalitet?

Avslutningsspørsmål:

- Ut fra det vi har snakket om, er det anen informasjon, andre synspunkter eller noe du ønsker å tilføye?
- Har du noen avsluttende tanker om forskningsprosjektet som du ønsker å dele?
- Er det i orden om jeg kontakter deg igjen dersom jeg har oppfølgingsspørsmål eller behov for å oppklare noe?